

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of: **Masayuki HATANAKA et al.**

Group Art Unit: 2136

Application Number: **10/069,112**

Examiner: **Pramila Parthasarathy**

Filed: **June 19, 2002**

Confirmation Number: **3705**

For: **DATA DISTRIBUTION SYSTEM AS WELL AS DATA SUPPLY DEVICE,
TERMINAL DEVICE AND RECORDING DEVICE FOR THE SAME**

Attorney Docket Number: **020231**

Customer Number: **38834**

SUBMISSION OF PRIORITY DOCUMENTS UNDER 35 U.S.C. 119

Mail Stop: AF
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

August 30, 2006

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

Japanese Patent Application No. JP1999-241747, filed on August 27, 1999; and

Japanese Patent Application No. JP1999-345229, filed on December 3, 1999.

In support of this claim, certified copies of the foreign application is attached herewith. Applicants request that the file of this application be marked to indicate that the applicants have complied with the requirements of 35 U.S.C. §119 and that the Patent Office kindly acknowledges receipt of said certified copies.

If any fees are required in connection with this paper, please charge Deposit Account No. 50-2866.

Respectfully submitted,
WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP

Lee C. Wright
Attorney for Applicants
Registration No. 41,441
Telephone: (202) 822-1100
Facsimile: (202) 822-1111

LCW/af

BEST AVAILABLE COPY

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1 9 9 9 年 1 2 月 3 日

出 願 番 号
Application Number:

平成 1 1 年 特 許 願 第 3 4 5 2 2 9 号

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号
the country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

J P 1 9 9 9 - 3 4 5 2 2 9

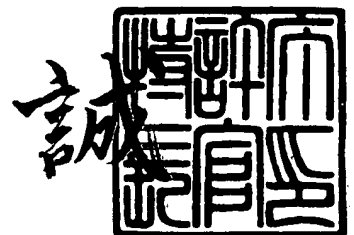
願 人
Applicant(s):

富士通株式会社
株式会社日立製作所
コロムビアミュージックエンタテインメント株式会社
三洋電機株式会社

2 0 0 6 年 8 月 2 2 日

特許庁長官
Commissioner,
Japan Patent Office

中 嶋



【書類名】 特許願

【整理番号】 1991488

【提出日】 平成11年12月 3日

【あて先】 特許庁長官殿

【国際特許分類】 H04M 11/08

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 畑中 正行

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 蒲田 順

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 畠山 卓久

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 長谷部 高行

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 小谷 誠剛

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号 富士通株式会社内

【氏名】 古田 茂樹

【発明者】

【住所又は居所】 東京都小平市上水本町 5 丁目 2 0 番 1 号 株式会社日立製作所 半導体グループ内

【氏名】 木下 泰三

【発明者】

【住所又は居所】 東京都港区赤坂四丁目 1 4 番 1 4 号 日本コロムビア株式会社内

【氏名】 穴澤 健明

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 日置 敏昭

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 金森 美和

【発明者】

【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号 三洋電機株式会社内

【氏名】 堀 吉宏

【特許出願人】

【識別番号】 000005223

【住所又は居所】 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

【氏名又は名称】 富士通株式会社

【特許出願人】

【識別番号】 000005108

【住所又は居所】 東京都千代田区神田駿河台 4 丁目 6 番地

【氏名又は名称】 株式会社日立製作所

【特許出願人】

【識別番号】 000004167
【住所又は居所】 東京都港区赤坂四丁目 1 4 番 1 4 号
【氏名又は名称】 日本コロムビア株式会社

【特許出願人】

【識別番号】 000001889
【住所又は居所】 大阪府守口市京阪本通 2 丁目 5 番 5 号
【氏名又は名称】 三洋電機株式会社

【代理人】

【識別番号】 100064746
【弁理士】
【氏名又は名称】 深見 久郎

【選任した代理人】

【識別番号】 100085132
【弁理士】
【氏名又は名称】 森田 俊雄

【選任した代理人】

【識別番号】 100091409
【弁理士】
【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781
【弁理士】
【氏名又は名称】 堀井 豊

【先の出願に基づく優先権主張】

【出願番号】 平成11年特許願第241747号
【出願日】 平成11年 8月27日

【手数料の表示】

【予納台帳番号】 008693

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 データ配信システム

【特許請求の範囲】

【請求項 1】 コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第 1 のインターフェース部と

前記暗号化コンテンツデータの通信ごとに更新される第 1 の共通鍵を生成する第 1 のセッションキー発生部と、

前記ユーザの端末に対応して予め定められた第 1 の公開暗号化鍵により前記第 1 の共通鍵を暗号化して前記第 1 のインターフェース部に与えるためのセッションキー暗号化部と、

前記第 1 の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、

前記暗号化コンテンツデータを復号するためのライセンスキーを、前記セッションキー復号部により復号されたデータを鍵データとして暗号化するための第 1 のライセンスデータ暗号化処理部と、

前記第 1 のライセンスデータ暗号化処理部の出力を第 2 の共通鍵でさらに暗号化して前記第 1 のインターフェース部に与え配信するための第 2 のライセンスデータ暗号化処理部とを備え、

各前記端末は、

外部との間でデータを授受するための第 2 のインターフェース部と、

前記暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、

前記配信データ解読部は、

前記第 1 の公開暗号化鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵を保持する第 1 の鍵保持部と、

前記第 1 の公開暗号化鍵によって暗号化された前記第 1 の共通鍵を受けて、復号処理するための第 1 の復号処理部と、

第 2 の公開暗号化鍵を保持するための第 2 の鍵保持部と、

前記第 2 の公開暗号化鍵を、前記第 1 の共通鍵に基づいて暗号化し、前記第 2 のインターフェース部に出力するための第 1 の暗号化処理部と、

前記第 2 のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、前記第 2 の共通鍵に基づいて復号化するための第 2 の復号処理部と、

前記第 2 の復号処理部の出力を受けて、格納するための第 1 の記憶部と、

前記第 2 の公開暗号化鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部と、

前記第 1 の記憶部に格納されたデータに基づいて、前記第 2 の秘密復号鍵により前記ライセンスキーを復号するための第 3 の復号処理部とを備える、データ配信システム。

【請求項 2】 前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第 1 の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた鍵であり、

前記第 2 の秘密復号鍵は、前記メモリカードごとに異なる、請求項 1 記載のデータ配信システム。

【請求項 3】 前記第 2 および第 3 の復号処理部は、前記コンテンツデータ供給装置において前記第 2 の公開暗号化鍵で暗号化され、さらに前記第 2 の共通鍵で暗号化されて、前記ライセンスキーとともに配信されるライセンス情報データを前記第 2 のインターフェース部を介して受け、前記第 2 の共通鍵および前記第 2 の秘密復号鍵に基づいて復号し、

前記配信データ解読部は、

復号された前記ライセンス情報データを格納する第 2 の記憶部をさらに備える、請求項 2 記載のデータ配信システム。

【請求項 4】 前記第 1 の共通鍵と前記第 2 の共通鍵とは、前記暗号化コンテンツデータの通信の際に、前記第 1 のセッションキー発生部により生成された同一の鍵データである、請求項 3 記載のデータ配信システム。

【請求項 5】 前記第 1 の記憶部は、前記ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格

納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第 1 の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記第 3 の復号処理部からの前記ライセンスキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、

前記第 1 の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第 3 の共通鍵を生成する第 2 のセッションキー発生部と、

前記配信データ解読部からの前記第 3 の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第 1 の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項 4 記載のデータ配信システム。

【請求項 6】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツキーおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、

前記第 2 の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第 3 の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第 3 の公開暗号化鍵を復号して抽出し、

前記第 2 の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記ライセンスキーおよび前記ライセンス情報データを前記第 3 の公開暗号化鍵で暗号化し、

前記第 1 の暗号化処理部は、前記第 2 の暗号化処理部の出力を受けて、前記第 3 の共通鍵に基づいて暗号化して前記第 2 のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第 2 の記憶部に格納されている前記ライセンス情報データを消去し、

前記第 1 の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 5 記載のデータ配信システム。

【請求項 7】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第 1 の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 5 記載のデータ配信システム。

【請求項 8】 前記配信データ解読部は、

前記第 2 の共通鍵を生成するための第 3 のセッションキー発生部と、

前記第 3 のセッションキー発生部の出力を暗号化して前記第 2 のインターフェース部に与えることが可能な第 3 の暗号化処理部とをさらに含む、請求項 3 記載のデータ配信システム。

【請求項 9】 前記第 1 の記憶部は、前記ライセンスキーに基づいて復号できる前記暗号化コンテンツデータを前記コンテンツデータ供給装置から受けて格納し、

前記配信データ解読部は、

外部から指示される再生動作モードに応じて、前記第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、前記配信データ解読部の動作を制御するための制御部をさらに備え、

前記第 3 の暗号化処理部は、第 4 の公開暗号化鍵により前記第 3 のセッションキー発生部の出力を暗号化して前記第 2 のインターフェース部に与え、

前記第 1 の暗号化処理部は、前記制御部に制御されて、前記コンテンツデータ

の再生動作が指示されるのに応じて、前記第 3 の復号処理部からの前記ライセンスキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、

前記第 1 の記憶部は、前記制御部に制御されて、前記コンテンツデータの再生動作が指示されるのに応じて、前記暗号化コンテンツデータを出力し、

各前記端末は、

前記暗号化コンテンツデータの通信ごとに更新される前記第 3 の共通鍵を生成する第 2 のセッションキー発生部と、

前記第 4 の公開暗号化鍵を前記配信データ解読部に与える公開鍵保持部と、

前記第 4 の公開暗号化鍵で暗号化された前記第 2 の共通鍵を復号可能な公開鍵復号部と、

前記配信データ解読部からの前記第 3 の共通鍵により暗号化された前記ライセンスキーを受けて復号して抽出し、前記第 1 の記憶部から出力された前記暗号化コンテンツデータを前記ライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える、請求項 8 記載のデータ配信システム。

【請求項 10】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータおよび前記ライセンス情報データを移転するための移動動作モードに応じて、前記配信データ解読部の動作を制御するための制御部と、

第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、

前記第 2 の復号処理部は、前記制御部に制御されて、前記移動動作モードが指定されるのに応じて、前記第 3 の共通鍵に基づいて暗号化されて前記他の端末の側から送信される前記第 3 の公開暗号化鍵を復号して抽出し、

前記第 2 の暗号化処理部は、前記移動動作モードが指定されるのに応じて、前記ライセンスキーおよび前記ライセンス情報データを前記第 3 の公開暗号化鍵で暗号化し、

前記第 1 の暗号化処理部は、前記第 2 の暗号化処理部の出力を受けて、前記第 3 の共通鍵に基づいて暗号化して前記第 2 のインターフェース部に与え、

前記制御部は、前記移動動作モードが指定されるのに応じて、前記第 2 の記憶

部に格納されている前記ライセンス情報データを消去し、

前記第 1 の記憶部は、前記移動動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 9 記載のデータ配信システム。

【請求項 1 1】 前記配信データ解読部は、

外部から指示される他の端末に前記暗号化コンテンツデータを移転するための複製動作モードに応じて、前記配信データ解読部の動作を制御するための制御部をさらに含み、

前記第 1 の記憶部は、前記複製動作モードが指定されるのに応じて、前記暗号化コンテンツデータを前記第 2 のインターフェース部に与える、請求項 9 記載のデータ配信システム。

【請求項 1 2】 前記第 1 のインターフェース部と前記第 2 のインターフェース部とは、携帯電話網により接続され、

前記コンテンツデータ供給装置は、

前記第 1 の公開暗号鍵に基づいて、前記ユーザの認証を行なう、請求項 1 記載のデータ配信システム。

【請求項 1 3】 前記第 1 のインターフェース部は、

前記端末と直接接続可能なコネクタ部を含む、請求項 1 記載のデータ配信システム。

【請求項 1 4】 前記第 1 のインターフェース部は、

前記メモリーカードと直接接続可能な接続部を含む、請求項 2 記載のデータ配信システム。

【請求項 1 5】 コンテンツデータ供給装置から、暗号化コンテンツデータと前記暗号化データを復号するためのコンテンツキーとのうちの少なくとも 1 つを複数のユーザの各端末に配信するためのデータ配信システムであって、

前記コンテンツデータ供給装置は、

外部との間でデータを授受するための第 1 のインターフェイス部と、

前記暗号化コンテンツデータの通信ごとに更新される第 1 の共通鍵を生成する第 1 のセッションキー発生部と、

前記ユーザの端末に対応して予め定められた第 1 の公開暗号化鍵により前記第 1 の共通鍵を暗号化して前記第 1 のインターフェイス部に与えるためのセッションキー暗号化処理部と、

前記第 2 の共通鍵により暗号化されて返信される第 2 の共通鍵と第 2 の公開暗号化鍵を復号し抽出するセッションキー復号部と、

前記暗号化コンテンツデータを復号するためのコンテンツキーを、前記セッションキー復号部により復号された第 2 の公開暗号化鍵により暗号化するための第 1 のライセンスデータ暗号化処理部と、

前記第 1 のライセンスデータ暗号化処理部の出力を前記第 2 の共通鍵でさらに暗号化して前記第 1 のインターフェイス部に与え配信するための第 2 のライセンス暗号化処理部とを備え、

各前記端末は、

外部との間でデータを授受するための第 2 のインターフェイス部と、

前記暗号化コンテンツデータおよび前記コンテンツキーを受けて格納する配信データ解読部とを備え、

前記配信データ解読部は、

前記第 1 の公開暗号化鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵を保持する第 1 の鍵保持部と、

前記第 1 の公開暗号化鍵によって暗号化された前記第 1 の共通鍵を受けて、復号処理するための第 1 の復号処理部と、

第 2 の公開暗号化鍵を保持するための第 2 の鍵保持部と、

第 2 の共通鍵を生成する第 2 のセッションキー発生部と、

前記第 2 の公開暗号化鍵と前記第 2 の共通鍵を、前記第 1 の共通鍵に基づいて暗号化し、前記第 2 のインターフェイス部に出力するための第 1 の暗号化処理部と、

前記第 2 のライセンスデータ暗号化処理部からの暗号化されたコンテンツキーを受け、前記第 2 の共通鍵に基づいて復号するための第 2 の復号処理部と、

前記第 2 の復号処理部の出力と、前記コンテンツキーにて復号可能な暗号化コンテンツデータを格納するための記憶部と、

前記第 2 の公開暗号化鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部と、

前記記憶部に格納されたデータに基づいて、前記第 2 の秘密復号鍵により前記コンテンツキーを復号し抽出するための第 3 の復号処理部と、

前記第 1 の公開暗号化鍵を少なくとも含む第 1 の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能な第 1 の認証データ保持部と、

前記公開認証鍵により復号できる外部から与えられる第 1 の認証データを復号して抽出するための第 1 の認証復号処理部とを備え、

前記コンテンツデータ供給部は、

前記第 1 の認証復号処理部により抽出された前記第 1 の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する配信制御手段をさらに含む、データ配信システム。

【請求項 1 6】 前記配信データ解読部は、前記端末に着脱可能なメモリカードであり、

前記第 1 の秘密復号鍵は、前記メモリカードの種類に対応して予め定められた値であり

前記第 2 の秘密復号鍵は、前記メモリカードごとに異なる、請求項 1 5 記載のデータ配信システム。

【請求項 1 7】 各前記端末は、コンテンツ再生部をさらに備え、

前記コンテンツ再生部は、

予め定められた第 3 の公開暗号化鍵を少なくとも含む第 2 の認証データを前記公開認証鍵に基づいて復号できるように暗号化して保持し、外部に対して出力できる第 2 の認証データ保持部をさらに含む、請求項 1 5 記載のデータ配信システム。

【請求項 1 8】 前記第 1 の認証復号処理部は、

前記公開認証鍵により復号できるように暗号化された第 2 の認証データをさらに復号して出力し、

前記配信制御部は、

前記第 1 の認証復号処理部にて抽出された前記第 1 の認証データおよび前記第 2 の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する、請求項 1 7 に記載のデータ配信システム。

【請求項 1 9】 前記第 1 のインタフェイス部と前記第 2 のインタフェイス部とは、携帯電話網により接続される、請求項 1 5 記載のデータ配信システム。

【請求項 2 0】 前記第 1 のインタフェイス部は、
前記端末と直接接続可能なコネクタ部を含む、請求項 1 5 記載のデータ配信システム。

【請求項 2 1】 前記第 1 のインタフェイス部は、
前記データ格納部と直接接続可能な接続部を含む、請求項 1 6 記載のデータ配信システム。

【請求項 2 2】 前記データ解読部は、
前記接続部からのデータを受ける複数の端子を含み、
外部からの指令に従って、前記接続部からデータを受ける端子数が切換え可能である、請求項 2 1 記載のデータ配信システム。

【請求項 2 3】 前記データ再生部は、
前記第 3 の公開暗号鍵にて暗号化されたデータを復号する第 3 の秘密復号鍵を保持するための第 4 の鍵保持部と、
外部にて前記第 3 の公開暗号化鍵によって暗号化された第 2 の共通鍵を復号し抽出するための第 3 の復号処理部と、

第 3 の共通鍵を生成する第 3 のセッションキー発生部と、
前記第 3 の復号処理部にて復号し抽出した前記第 2 の共通鍵に基づいて、前記第 3 の共通鍵を暗号化し出力するための第 2 の暗号化処理部と、

外部にて前記第 3 の共通鍵に基づいて暗号化されたコンテンツキーを復号し抽出するための第 4 復号処理部と、

前記記録部に記録された暗号化コンテンツデータを抽出した前記コンテンツキーにて復号し、再生するためのデータ再生部とをさらに備え、

配信データ解読部は、

前記公開認証鍵により復号できる前記コンテンツ再生部からの与えられる暗号

化された第 2 の認証データを復号して前記第 3 の公開鍵を抽出するための第 2 の認証復号処理部と、

前記第 2 のセッションキー発生部にて生成した第 2 の共通鍵を前記第 3 の公開暗号化鍵に基づいて暗号化する第 3 の暗号化処理部と、

前記データ再生部にて前記第 2 の共通鍵にて暗号化された前記第 3 の共通鍵を受けて、前記第 1 の復号処理部にて前記第 2 の共通鍵に基づいて復号した前記第 3 の共通鍵に基づいて、前記記録部に格納されたデータを前記第 2 の秘密復号鍵にて復号した前記コンテンツキーを、前記第 1 の暗号化処理部にて暗号化し、前記コンテンツ再生部へ出力を指示する制御部とをさらに備え、

前記制御手段は、前記第 2 の認証復号処理部により復号された前記第 2 の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する、請求項 1 7 記載のデータ配信システム。

【請求項 2 4】 前記配信データ解読部は、

前記第 2 の公開鍵によって前記第 2 の共通鍵を暗号化するための第 4 の暗号化処理部をさらに含み、

前記認証復号処理部は、外部から指示される、他の配信データ解読部に少なくとも前記コンテンツキーを移転する移動処理に応じて、前記他のデータ解読部の前記公開認証鍵によって復号できる暗号化された第 1 の認証データを、前記公開認証鍵にて復号して、前記他のデータ解読部における第 1 の公開暗号化鍵を抽出し、

前記第 2 のセッションキー発生部は、前記移動処理に応じて、前記第 2 の共通鍵を発生し、

前記第 3 の暗号化処理部は、前記移動処理に応じて、前記他の配信データ解読部の第 1 の公開暗号化鍵に基づいて、前記第 2 の共通鍵を暗号化し、

前記第 2 の復号処理部は、前記移動処理に応じて、前記他の配信データ解読部から前記第 2 の共通鍵によって暗号化され、入力される第 4 の共通鍵と他の配信データ解読部の第 2 の公開暗号化鍵とを復号して抽出し、

前記第 3 の復号処理部は、前記移動処理に応じて、第 2 の秘密復号鍵に基づいて、前記記録部に格納された第 2 の公開暗号化鍵にて暗号化されたデータを復号

し、コンテンツキーを抽出し、

前記第 4 の暗号化処理部は、前記移動処理に応じて、前記他のメモリカードの第 2 の公開暗号化鍵に基づいて、抽出された前記コンテンツキーを暗号化し、

前記第 1 の暗号化処理部は、前記移動処理に応じて、前記第 4 の暗号化処理部の出力を前記第 4 の共通鍵にて暗号化し、前記他の配信データ解読部に対して出力し、

前記制御手段は、前記第 2 の認証復号処理部により抽出された前記他のデータ解読部から出力された第 2 の認証データに基づき認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する、請求項 1 6 記載のデータ配信システム。

【請求項 2 5】 前記配信データ解読部は、

前記認証復号処理は、外部から指示される、他の配信データ解読部から少なくとも前記コンテンツキーを移転する移動受理処理に応じて、前記第 2 の認証データ保持部が前記第 2 の認証データを出力し、

前記第 1 の復号処理部は、前記移動受理処理に応じて、前記他の配信データ解読部から前記第 1 の公開暗号化鍵によって暗号化され、入力される前記他の配信データ解読部にて発生された前記第 4 の共通鍵を復号して抽出し、

前記第 2 のセッションキー発生部は、前記移動受理処理に応じて、第 2 の共通鍵を発生し、

前記第 1 の暗号化処理部は、前記移動受理処理に応じて、第 4 の共通鍵に基づいて、前記第 2 の公開暗号化鍵と前記第 2 の共通鍵とを暗号化して出力し、

前記第 2 の復号処理部は、前記他の配信データ解読部に前記第 2 の公開暗号化鍵にて暗号化され、さらに前記第 2 の共通鍵にて暗号化されたコンテンツキーを前記第 2 の共通鍵にて復号し、前記記録部に記録する請求項 2 2 記載のデータ配信システム。

【請求項 2 6】 前記コンテンツデータ供給装置は、

前記コンテンツ再生部と共通な第 5 の共通鍵を保持する第 5 の鍵保持部と、

前記第 5 の鍵保持部に保持された前記第 5 の共通鍵に基づいて、前記コンテンツキーを暗号化し前記第 1 のライセンス暗号化処理部に対して出力する第 3 のラ

イセンス暗号化部をさらに含み、

前記コンテンツ再生部は、

前記第 5 の共通鍵を保持する第 6 の鍵保持手段と、

前記第 4 の復号処理部と前記データ再生部との間に設けられ、前記第 6 の鍵保持部に保持された前記第 5 の共通鍵によって、前記第 4 の復号処理部の出力から前記コンテンツキーを復号し抽出し、前記データ再生部に対して出力する第 5 の復号処理部をさらに含む、請求項 2 1 記載のデータ配信システム。

【請求項 2 7】 前記コンテンツデータ供給装置は、

前記コンテンツ再生部にて復号可能な第 4 の公開暗号化鍵を保持する第 5 の鍵保持部と、

第 4 の公開暗号化鍵に基づいて前記コンテンツキーを暗号化し前記第 1 のライセンス暗号化処理部にて出力する第 3 のライセンス暗号化部をさらに含み、

前記コンテンツ再生部は、

第 4 の公開暗号化鍵によって暗号化されたデータを復号できる第 4 の秘密復号鍵を保持する第 6 の鍵保持手段と、

前記第 4 の復号処理部と前記データ再生部との間に設けられ、第 4 の秘密復号鍵によって前記第 4 の復号処理部の出力から前記コンテンツキーを復号し抽出し、前記データ再生部に対して出力する第 5 の復号処理部をさらに含む、請求項 2 1 記載のデータ配信システム。

【請求項 2 8】 前記データ再生部は、

複数の配信データ解読部を備える、請求項 1 6 記載のデータ配信システム。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、携帯電話等の端末に対して情報を配送するためのデータ配信システムに関し、より特定的には、コピーされた情報に対する著作権保護を可能とするデータ配信システムに関するものである。

【0 0 0 2】

【従来の技術】

近年、インターネット等の情報通信網等の進歩により、携帯電話等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【0 0 0 3】

このような情報通信においてはデジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像情報を各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、情報のコピーを行なうことが可能である。

【0 0 0 4】

したがって、このような情報通信網上において、音楽情報や画像情報等の著作権の存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【0 0 0 5】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物の複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【0 0 0 6】

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタル情報を記録した記録媒体を例にとって考えてみると、通常販売されている音楽情報を記録したCD（コンパクトディスク）については、CDから光磁気ディスク（MD等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やMD等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

【0 0 0 7】

しかも、CDからMDへデジタル信号である音楽情報をコピーした場合、これらの情報がコピー劣化のほとんどないデジタル情報であることに鑑み、1つのMDからさらに他のMDに音楽データをデジタル情報としてコピーすることは、著

著作権保護のために機器の構成上できないようになっている。

【0 0 0 8】

すなわち、現状においては、デジタル記録媒体であるCDからMDへのコピーは、親から子へのコピーは自由に行なうことができるものの、記録可能なMDからMDへのコピーを行なうことはできない。

【0 0 0 9】

【発明が解決しようとする課題】

そのような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【0 0 1 0】

この場合、情報通信網を通じて公衆に送信される著作物データを、本来受信する権限のないユーザが受信することを防止する必要があるのはもちろんのこと、仮に権限を有するユーザが受信を行なった場合でも、一度受信された著作物が、さらに勝手に複製されることを防止することも必要となる。

【0 0 1 1】

本発明は、上記のような問題点を解決するためになされたものであって、その目的は、情報通信網、たとえば携帯電話等の情報通信網を介して著作物データを配信する場合に、正当なアクセス権を有するユーザのみがこのような情報を受信することが可能な情報配信システムを提供することである。

【0 0 1 2】

この発明の他の目的は、配信された著作物データが、著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供することである。

【0 0 1 3】

【課題を解決するための手段】

請求項1記載のデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータを複数のユーザの各端末に配信するためのデータ配信システムであって、コンテンツデータ供給装置は、外部との間でデータを授受するための第1のインターフェース部と暗号化コンテンツデータの通信ごとに更新される

第 1 の共通鍵を生成する第 1 のセッションキー発生部と、ユーザの端末に対応して予め定められた第 1 の公開暗号化鍵により第 1 の共通鍵を暗号化して第 1 のインターフェース部に与えるためのセッションキー暗号化部と、第 1 の共通鍵により暗号化されて返信されるデータを復号するためのセッションキー復号部と、暗号化コンテンツデータを復号するためのライセンスキーを、セッションキー復号部により復号されたデータを鍵データとして暗号化するための第 1 のライセンスデータ暗号化処理部と、第 1 のライセンスデータ暗号化処理部の出力を第 2 の共通鍵でさらに暗号化して第 1 のインターフェース部に与え配信するための第 2 のライセンスデータ暗号化処理部とを備え、各端末は、外部との間でデータを授受するための第 2 のインターフェース部と、暗号化コンテンツデータを受けて格納する配信データ解読部とを備え、配信データ解読部は、第 1 の公開暗号化鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵を保持する第 1 の鍵保持部と、第 1 の公開暗号化鍵によって暗号化された第 1 の共通鍵を受けて、復号処理するための第 1 の復号処理部と、第 2 の公開暗号化鍵を保持するための第 2 の鍵保持部と、第 2 の公開暗号化鍵を、第 1 の共通鍵に基づいて暗号化し、第 2 のインターフェース部に出力するための第 1 の暗号化処理部と、第 2 のライセンスデータ暗号化処理部からの暗号化されたライセンスキーを受け、第 2 の共通鍵に基づいて復号化するための第 2 の復号処理部と、第 2 の復号処理部の出力を受けて、格納するための第 1 の記憶部と、第 2 の公開暗号化鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部と、第 1 の記憶部に格納されたデータに基づいて、第 2 の秘密復号鍵によりライセンスキーを復号するための第 3 の復号処理部とを備える。

【0014】

請求項 2 記載のデータ配信システムは、請求項 1 記載のデータ配信システムの構成に加えて、配信データ解読部は、端末に着脱可能なメモリカードであり、第 1 の秘密復号鍵は、メモリカードの種類に対応して予め定められた鍵であり、第 2 の秘密復号鍵は、メモリカードごとに異なる。

【0015】

請求項 3 記載のデータ配信システムは、請求項 2 記載のデータ配信システムの

構成に加えて、第 2 および第 3 の復号処理部は、コンテンツデータ供給装置において第 2 の公開暗号化鍵で暗号化され、さらに第 2 の共通鍵で暗号化されて、ライセンスキーとともに配信されるライセンス情報データを第 2 のインターフェース部を介して受け、第 2 の共通鍵および第 2 の秘密復号鍵に基づいて復号し、配信データ解読部は、復号されたライセンス情報データを格納する第 2 の記憶部をさらに備える。

【0 0 1 6】

請求項 4 記載のデータ配信システムは、請求項 3 記載のデータ配信システムの構成に加えて、第 1 の共通鍵と第 2 の共通鍵とは、暗号化コンテンツデータの通信の際に、第 1 のセッションキー発生部により生成された同一の鍵データである。

【0 0 1 7】

請求項 5 記載のデータ配信システムは、請求項 4 記載のデータ配信システムの構成に加えて、第 1 の記憶部は、ライセンスキーに基づいて復号できる暗号化コンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読部は、外部から指示される再生動作モードに応じて、第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第 1 の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第 3 の復号処理部からのライセンスキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、第 1 の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第 3 の共通鍵を生成する第 2 のセッションキー発生部と、配信データ解読部からの第 3 の共通鍵により暗号化されたライセンスキーを受けて復号して抽出し、第 1 の記憶部から出力された暗号化コンテンツデータをライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

【0 0 1 8】

請求項 6 記載のデータ配信システムは、請求項 5 記載のデータ配信システムの

構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツキーおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、第 2 の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第 3 の共通鍵に基づいて暗号化されて他の端末の側から送信される第 3 の公開暗号化鍵を復号して抽出し、第 2 の暗号化処理部は、移動動作モードが指定されるのに応じて、ライセンスキーおよびライセンス情報データを第 3 の公開暗号化鍵で暗号化し、第 1 の暗号化処理部は、第 2 の暗号化処理部の出力を受けて、第 3 の共通鍵に基づいて暗号化して第 2 のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第 2 の記憶部に格納されているライセンス情報データを消去し、第 1 の記憶部は、移動動作モードが指定されるのに応じて、暗号化コンテンツデータを第 2 のインターフェース部に与える。

【 0 0 1 9 】

請求項 7 記載のデータ配信システムは、請求項 5 記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第 1 の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第 2 のインターフェース部に与える。

【 0 0 2 0 】

請求項 8 記載のデータ配信システムは、請求項 3 記載のデータ配信システムの構成に加えて、配信データ解読部は、第 2 の共通鍵を生成するための第 3 のセッションキー発生部と、第 3 のセッションキー発生部の出力を暗号化して第 2 のインターフェース部に与えることが可能な第 3 の暗号化処理部とをさらに含む。

【 0 0 2 1 】

請求項 9 記載のデータ配信システムは、請求項 8 記載のデータ配信システムの構成に加えて、第 1 の記憶部は、ライセンスキーに基づいて復号できる暗号化コンテンツデータをコンテンツデータ供給装置から受けて格納し、配信データ解読

部は、外部から指示される再生動作モードに応じて、第 2 の記憶部に格納されたライセンス情報データにより再生可能かを判断して、配信データ解読部の動作を制御するための制御部をさらに備え、第 3 の暗号化処理部は、第 4 の公開暗号化鍵により第 3 のセッションキー発生部の出力を暗号化して第 2 のインターフェース部に与え、第 1 の暗号化処理部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、第 3 の復号処理部からのライセンスキーを受けて、第 3 の共通鍵に基づいて暗号化して出力し、第 1 の記憶部は、制御部に制御されて、コンテンツデータの再生動作が指示されるのに応じて、暗号化コンテンツデータを出力し、各端末は、暗号化コンテンツデータの通信ごとに更新される第 3 の共通鍵を生成する第 2 のセッションキー発生部と、第 4 の公開暗号化鍵を配信データ解読部に与える公開鍵保持部と、第 4 の公開暗号化鍵で暗号化された第 2 の共通鍵を復号可能な公開鍵復号部と、配信データ解読部からの第 3 の共通鍵により暗号化されたライセンスキーを受けて復号して抽出し、第 1 の記憶部から出力された暗号化コンテンツデータをライセンスキーにより復号して再生するコンテンツデータ再生部とをさらに備える。

【 0 0 2 2 】

請求項 1 0 記載のデータ配信システムは、請求項 9 記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータおよびライセンス情報データを移転するための移動動作モードに応じて、配信データ解読部の動作を制御するための制御部と、第 3 の公開暗号化鍵で暗号化処理を行なうための第 2 の暗号化処理部とをさらに含み、第 2 の復号処理部は、制御部に制御されて、移動動作モードが指定されるのに応じて、第 3 の共通鍵に基づいて暗号化されて他の端末の側から送信される第 3 の公開暗号化鍵を復号して抽出し、第 2 の暗号化処理部は、移動動作モードが指定されるのに応じて、ライセンスキーおよびライセンス情報データを第 3 の公開暗号化鍵で暗号化し、第 1 の暗号化処理部は、第 2 の暗号化処理部の出力を受けて、第 3 の共通鍵に基づいて暗号化して第 2 のインターフェース部に与え、制御部は、移動動作モードが指定されるのに応じて、第 2 の記憶部に格納されているライセンス情報データを消去し、第 1 の記憶部は、移動動作モードが指定されるのに応じて、

暗号化コンテンツデータを第 2 のインターフェース部に与える。

【 0 0 2 3 】

請求項 1 1 記載のデータ配信システムは、請求項 9 記載のデータ配信システムの構成に加えて、配信データ解読部は、外部から指示される他の端末に暗号化コンテンツデータを移転するための複製動作モードに応じて、配信データ解読部の動作を制御するための制御部をさらに含み、第 1 の記憶部は、複製動作モードが指定されるのに応じて、暗号化コンテンツデータを第 2 のインターフェース部に与える。

【 0 0 2 4 】

請求項 1 2 記載のデータ配信システムは、請求項 1 記載のデータ配信システムの構成に加えて、第 1 のインターフェース部と第 2 のインターフェース部とは、携帯電話網により接続され、コンテンツデータ供給装置は、第 1 の公開暗号鍵に基づいて、ユーザの認証を行なう。

【 0 0 2 5 】

請求項 1 3 記載のデータ配信システムは、請求項 1 記載のデータ配信システムの構成に加えて、第 1 のインターフェース部は、端末と直接接続可能なコネクタ部を含む。

【 0 0 2 6 】

請求項 1 4 記載のデータ配信システムは、請求項 2 記載のデータ配信システムの構成に加えて、第 1 のインターフェース部は、メモリーカードと直接接続可能な接続部を含む。

【 0 0 2 7 】

請求項 1 5 記載のデータ配信システムは、コンテンツデータ供給装置から、暗号化コンテンツデータと暗号化データを復号するためのコンテンツキーとのうちの少なくとも 1 つを複数のユーザの各端末に配信するためのデータ配信システムであって、コンテンツデータ供給装置は、外部との間でデータを授受するための第 1 のインターフェイス部と、暗号化コンテンツデータの通信ごとに更新される第 1 の共通鍵を生成する第 1 のセッションキー発生部と、ユーザの端末に対応して予め定められた第 1 の公開暗号化鍵により第 1 の共通鍵を暗号化して第 1 のイ

ンターフェイス部に与えるためのセッションキー暗号化処理部と、第 2 の共通鍵により暗号化されて返信される第 2 の共通鍵と第 2 の公開暗号化鍵を復号し抽出するセッションキー復号部と、暗号化コンテンツデータを復号するためのコンテンツキーを、セッションキー復号部により復号された第 2 の公開暗号化鍵により暗号化するための第 1 のライセンスデータ暗号化処理部と、第 1 のライセンスデータ暗号化処理部の出力を第 2 の共通鍵でさらに暗号化して第 1 のインターフェイス部に与え配信するための第 2 のライセンス暗号化処理部とを備え、各端末は、外部との間でデータを授受するための第 2 のインターフェイス部と、暗号化コンテンツデータおよびコンテンツキーを受けて格納する配信データ解読部とを備え、配信データ解読部は、第 1 の公開暗号化鍵によって暗号化されたデータを復号化するための第 1 の秘密復号鍵を保持する第 1 の鍵保持部と、第 1 の公開暗号化鍵によって暗号化された第 1 の共通鍵を受けて、復号処理するための第 1 の復号処理部と、第 2 の公開暗号化鍵を保持するための第 2 の鍵保持部と、第 2 の共通鍵を生成する第 2 のセッションキー発生部と、第 2 の公開暗号化鍵と第 2 の共通鍵を、第 1 の共通鍵に基づいて暗号化し、第 2 のインターフェイス部に出力するための第 1 の暗号化処理部と、第 2 のライセンスデータ暗号化処理部からの暗号化されたコンテンツキーを受け、第 2 の共通鍵に基づいて復号するための第 2 の復号処理部と、第 2 の復号処理部の出力と、コンテンツキーにて復号可能な暗号化コンテンツデータを格納するための記憶部と、第 2 の公開暗号化鍵によって暗号化されたデータを復号化するための第 2 の秘密復号鍵を保持する第 3 の鍵保持部と、記憶部に格納されたデータに基づいて、第 2 の秘密復号鍵によりコンテンツキーを復号し抽出するための第 3 の復号処理部と、第 1 の公開暗号化鍵を少なくとも含む第 1 の認証データを公開認証鍵により復号できるように暗号化して保持し外部に出力可能な第 1 の認証データ保持部と、公開認証鍵により復号できる外部から与えられる第 1 の認証データを復号して抽出するための第 1 の認証復号処理部とを備え、コンテンツデータ供給部は、第 1 の認証復号処理部により抽出された第 1 の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する配信制御手段をさらに含む。

【 0 0 2 8 】

請求項 1 6 記載のデータ配信システムは、請求項 1 5 記載のデータ配信システムの構成に加えて、配信データ解読部は、端末に着脱可能なメモリカードであり、第 1 の秘密復号鍵は、メモリカードの種類に対応して予め定められた値であり、第 2 の秘密復号鍵は、メモリカードごとに異なる。

【 0 0 2 9 】

請求項 1 7 記載のデータ配信システムは、請求項 1 5 記載のデータ配信システムの構成に加えて、各端末は、コンテンツ再生部をさらに備え、コンテンツ再生部は、予め定められた第 3 の公開暗号鍵を少なくとも含む第 2 の認証データを公開認証鍵に基づいて復号できるように暗号化して保持し、外部に対して出力できる第 2 の認証データ保持部をさらに含む。

【 0 0 3 0 】

請求項 1 8 記載のデータ配信システムは、請求項 1 7 記載のデータ配信システムの構成に加えて、第 1 の認証復号処理部は、公開認証鍵により復号できるように暗号化された第 2 の認証データをさらに復号して出力し、配信制御部は、第 1 の認証復号処理部にて抽出された第 1 の認証データおよび第 2 の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを配信するか否かを判断する。

【 0 0 3 1 】

請求項 1 9 記載のデータ配信システムは、請求項 1 5 記載のデータ配信システムの構成に加えて、第 1 のインタフェイス部と第 2 のインタフェイス部とは、携帯電話網により接続される。

【 0 0 3 2 】

請求項 2 0 記載のデータ配信システムは、請求項 1 5 記載のデータ配信システムの構成に加えて、第 1 のインタフェイス部は、端末と直接接続可能なコネクタ部を含む。

【 0 0 3 3 】

請求項 2 1 記載のデータ配信システムは、請求項 1 6 記載のデータ配信システムの構成に加えて、第 1 のインタフェイス部は、データ格納部と直接接続可能な接続部を含む。

【 0 0 3 4 】

請求項 2 2 記載のデータ配信システムは、請求項 2 1 記載のデータ配信システムの構成に加えて、データ解読部は、接続部からのデータを受ける複数の端子を含み、外部からの指令に従って、接続部からデータを受ける端子数が切換え可能である。

【 0 0 3 5 】

請求項 2 3 記載のデータ配信システムは、請求項 1 7 記載のデータ配信システムの構成に加えて、データ再生部は、第 3 の公開暗号鍵にて暗号化されたデータを復号する第 3 の秘密復号鍵を保持するための第 4 の鍵保持部と、外部にて第 3 の公開暗号化鍵によって暗号化された第 2 の共通鍵を復号し抽出するための第 3 の復号処理部と、第 3 の共通鍵を生成する第 3 のセッションキー発生部と、第 3 の復号処理部にて復号し抽出した第 2 の共通鍵に基づいて、第 3 の共通鍵を暗号化し出力するための第 2 の暗号化処理部と、外部にて第 3 の共通鍵に基づいて暗号化されたコンテンツキーを復号し抽出するための第 4 復号処理部と、記録部に記録された暗号化コンテンツデータを抽出したコンテンツキーにて復号し、再生するためのデータ再生部とをさらに備え、配信データ解読部は、公開認証鍵により復号できるコンテンツ再生部からの与えられる暗号化された第 2 の認証データを復号して第 3 の公開鍵を抽出するための第 2 の認証復号処理部と、第 2 のセッションキー発生部にて生成した第 2 の共通鍵を第 3 の公開暗号化鍵に基づいて暗号化する第 3 の暗号化処理部と、データ再生部にて第 2 の共通鍵にて暗号化された第 3 の共通鍵を受けて、第 1 の復号処理部にて第 2 の共通鍵に基づいて復号した第 3 の共通鍵に基づいて、記録部に格納されたデータを第 2 の秘密復号鍵にて復号したコンテンツキーを、第 1 の暗号化処理部にて暗号化し、コンテンツ再生部へ出力を指示する制御部とをさらに備え、制御手段は、第 2 の認証復号処理部により復号された第 2 の認証データに基づいて認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する。

【 0 0 3 6 】

請求項 2 4 記載のデータ配信システムは、請求項 1 6 記載のデータ配信システムの構成に加えて、配信データ解読部は、第 2 の公開鍵によって第 2 の共通鍵を

暗号化するための第 4 の暗号化処理部をさらに含み、認証復号処理部は、外部から指示される、他の配信データ解読部に少なくともコンテンツキーを移転する移動処理に応じて、他のデータ解読部の公開認証鍵によって復号できる暗号化された第 1 の認証データを、公開認証鍵にて復号して、他のデータ解読部における第 1 の公開暗号化鍵を抽出し、第 2 のセッションキー発生部は、移動処理に応じて、第 2 の共通鍵を発生し、第 3 の暗号化処理部は、移動処理に応じて、他の配信データ解読部の第 1 の公開暗号化鍵に基づいて、第 2 の共通鍵を暗号化し、第 2 の復号処理部は、移動処理に応じて、他の配信データ解読部から第 2 の共通鍵によって暗号化され、入力される第 4 の共通鍵と他の配信データ解読部の第 2 の公開暗号化鍵とを復号して抽出し、第 3 の復号処理部は、移動処理に応じて、第 2 の秘密復号鍵に基づいて、記録部に格納された第 2 の公開暗号化鍵にて暗号化されたデータを復号し、コンテンツキーを抽出し、第 4 の暗号化処理部は、移動処理に応じて、他のメモリカードの第 2 の公開暗号化鍵に基づいて、抽出されたコンテンツキーを暗号化し、第 1 の暗号化処理部は、移動処理に応じて、第 4 の暗号化処理部の出力を第 4 の共通鍵にて暗号化し、他の配信データ解読部に対して出力し、制御手段は、第 2 の認証復号処理部により抽出された他のデータ解読部から出力された第 2 の認証データに基づき認証処理を行ない、少なくともコンテンツキーを出力するか否かを判断する。

【0 0 3 7】

請求項 2 5 記載のデータ配信システムは、請求項 2 2 記載のデータ配信システムの構成に加えて、配信データ解読部は、認証復号処理は、外部から指示される、他の配信データ解読部から少なくともコンテンツキーを移転する移動受理処理に応じて、第 2 の認証データ保持部が第 2 の認証データを出力し、第 1 の復号処理部は、移動受理処理に応じて、他の配信データ解読部から第 1 の公開暗号化鍵によって暗号化され、入力される他の配信データ解読部にて発生された第 4 の共通鍵を復号して抽出し、第 2 のセッションキー発生部は、移動受理処理に応じて、第 2 の共通鍵を発生し、第 1 の暗号化処理部は、移動受理処理に応じて、第 4 の共通鍵に基づいて、第 2 の公開暗号化鍵と第 2 の共通鍵とを暗号化して出力し、第 2 の復号処理部は、他の配信データ解読部に第 2 の公開暗号化鍵にて暗号化

され、さらに第 2 の共通鍵にて暗号化されたコンテンツキーを第 2 の共通鍵にて復号し、記録部に記録する。

【0 0 3 8】

請求項 2 6 記載のデータ配信システムは、請求項 2 1 記載のデータ配信システムの構成に加えて、コンテンツデータ供給装置は、コンテンツ再生部と共通な第 5 の共通鍵を保持する第 5 の鍵保持部と、第 5 の鍵保持部に保持された第 5 の共通鍵に基づいて、コンテンツキーを暗号化し第 1 のライセンス暗号化処理部に対して出力する第 3 のライセンス暗号化部をさらに含み、コンテンツ再生部は、第 5 の共通鍵を保持する第 6 の鍵保持手段と、第 4 の復号処理部とデータ再生部との間に設けられ、第 6 の鍵保持部に保持された第 5 の共通鍵によって、第 4 の復号処理部の出力からコンテンツキーを復号し抽出し、データ再生部に対して出力する第 5 の復号処理部をさらに含む。

【0 0 3 9】

請求項 2 7 記載のデータ配信システムは、請求項 2 1 記載のデータ配信システムの構成に加えて、コンテンツデータ供給装置は、コンテンツ再生部にて復号可能な第 4 の公開暗号化鍵を保持する第 5 の鍵保持部と、第 4 の公開暗号化鍵に基づいてコンテンツキーを暗号化し第 1 のライセンス暗号化処理部にて出力する第 3 のライセンス暗号化部をさらに含み、コンテンツ再生部は、第 4 の公開暗号化鍵によって暗号化されたデータを復号できる第 4 の秘密復号鍵を保持する第 6 の鍵保持手段と、第 4 の復号処理部とデータ再生部との間に設けられ、第 4 の秘密復号鍵によって第 4 の復号処理部の出力からコンテンツキーを復号し抽出し、データ再生部に対して出力する第 5 の復号処理部をさらに含む。

【0 0 4 0】

請求項 2 8 記載のデータ配信システムは、請求項 1 6 記載のデータ配信システムの構成に加えて、データ再生部は、複数の配信データ解読部を備える。

【0 0 4 1】

【発明の実施の形態】

[実施の形態 1]

[システムの全体構成]

図 1 は、本発明の情報配信システムの全体構成を概略的に説明するための概念図である。

【0 0 4 2】

なお、以下では携帯電話網を介して、音楽データを各ユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物データ、たとえば画像データ等の著作物データを、他の情報通信網を介して配信する場合にも適用することが可能なものである。

【0 0 4 3】

図 1 を参照して、著作権の存在する音楽情報を管理する配信サーバ 1 0 は、所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化したうえで、情報を配信するための配信キャリア 2 0 である携帯電話会社に、このような暗号化データを与える。一方、認証サーバ 1 2 は、音楽データの配信を求めてアクセスしてきた機器が正規の機器であるか否かの認証を行なう。

【0 0 4 4】

配信キャリア 2 0 は、自己の携帯電話網を通じて、各ユーザからの配信要求（配信リクエスト）を配信サーバ 1 0 に中継する。配信サーバ 1 0 は、配線リクエストがあると、認証サーバ 1 2 により正規の機器からのアクセスであることを確認し、要求されたコンテンツデータをさらに暗号化したうえで、配信キャリア 2 0 の携帯電話網を介して、各ユーザの携帯電話機に対して配信する。

【0 0 4 5】

図 1 においては、たとえば携帯電話ユーザ 1 の携帯電話機 1 0 0 には、携帯電話機 1 0 0 により受信された暗号化コンテンツデータを受取って、上記送信にあたって行なわれた暗号化については復号化したうえで、携帯電話機 1 0 0 中の音楽再生部（図示せず）に与えるための着脱可能なメモリカード 1 1 0 に格納する構成となっている。

【0 0 4 6】

さらに、たとえばユーザ 1 は、携帯電話機 1 0 0 に接続したヘッドホン 1 3 0 等を介してこのようなコンテンツデータを再生した音楽を聴取することが可能で

ある。

【0 0 4 7】

以下では、このような配信サーバ 1 0 と認証サーバ 1 2 と配信キャリア 2 0 とを併せて、音楽サーバ 3 0 と総称することにする。

【0 0 4 8】

また、このような音楽サーバ 3 0 から、各携帯電話端末等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0 0 4 9】

このような構成とすることで、まず、正規のメモリカードであるメモリカード 1 1 0 を購入していない正規のユーザでないものは、音楽サーバ 3 0 からの配信データを受取って再生することが困難な構成となる。

【0 0 5 0】

しかも、配信キャリア 2 0 において、たとえば 1 曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア 2 0 が携帯電話の通話料金として徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0 0 5 1】

しかも、このようなコンテンツデータの配信は、携帯電話網というクローズドなシステムを介して行なわれるため、インターネット等のオープンなシステムに比べて、著作権保護の対策を講じやすいという利点がある。

【0 0 5 2】

このとき、たとえばメモリカード 1 1 2 を有するユーザ 2 が、自己の携帯電話機 1 0 2 により、音楽サーバ 3 0 から直接コンテンツデータの配信を受けることは可能である。しかしながら、相当量の情報量を有するコンテンツデータ等をユーザ 2 が直接音楽サーバ 3 0 から受信することとすると、その受信のために比較的長い時間を要してしまう場合がある。このような場合、既に当該コンテンツデータの配信を受けているユーザ 1 から、そのコンテンツデータをコピーできることを可能としておけば、ユーザにとっての利便性が向上する。

【0 0 5 3】

しかしながら、著作権者の権利保護の観点からは、自由なコンテンツデータのコピーを放任することはシステム構成上許されない。

【0 0 5 4】

図 1 に示した例では、ユーザ 1 が受信したコンテンツデータを、コンテンツデータそのものおよび当該コンテンツデータを再生可能とするために必要な情報とともに、ユーザ 2 に対してコピーさせる場合をコンテンツデータの「移動」と呼ぶ。この場合、ユーザ 1 は、再生のために必要な情報（再生情報）ごとユーザ 2 にコピーさせるため、情報の移動を行なった後には、ユーザ 1 においてはコンテンツデータの再生を行なうことは不可能とする必要がある。ここで、コンテンツデータは所定の暗号化方式にしたがって暗号化された暗号化コンテンツデータとして配信され、「再生情報」とは、後に説明するように、上記所定の暗号化方式にしたがって暗号化コンテンツデータを復号可能なライセンスキーとも称する）と、著作権保護に関わる情報であるライセンス ID データやユーザ ID データ等のライセンス情報とを意味する。

【0 0 5 5】

これに対して、コンテンツデータのみを暗号化されたままの状態、ユーザ 2 にコピーさせることを音楽情報の「複製」と呼ぶこととする。

【0 0 5 6】

この場合、ユーザ 2 の端末には、このようなコンテンツデータを再生させるために必要な再生情報はコピーされない、ユーザ 2 は、暗号化コンテンツデータを得ただけでは、音楽を再生させることができない。したがって、ユーザ 2 が、このような音楽の再生を望む場合は、改めて音楽サーバ 3 0 からコンテンツデータの再生を可能とするための再生情報の配信を受ける必要がある。しかしながら、この場合は、再生を可能とするための情報の配信のみを受ければよい、ユーザ 2 が直接音楽サーバ 3 0 からすべての配信を受ける場合に比べて、格段に短い通話時間で、音楽再生を可能とすることができる。

【0 0 5 7】

たとえば、携帯電話機 1 0 0 および 1 0 2 が、P H S (Personal Handy Phone

）である場合には、いわゆるトランシーバモードの通話が可能となっているので、このような機能を利用して、ユーザ 1 からユーザ 2 への一括した情報の移転（移動）や、暗号化したコンテンツデータのみの転送（複製）を行なうことが可能である。

【0058】

図 1 に示したような構成においては、暗号化して配信されるコンテンツデータをユーザ側で再生可能とするためにシステム上必要とされるのは、第 1 には、通信における暗号化キー（鍵）を配送するための方式であり、さらに第 2 には、配信データを暗号化する方式そのものであり、さらに、第 3 には、このようにして配信されたデータの無断コピーを防止するためのデータ保護を実現する構成である。

【0059】

[暗号／復号鍵の構成]

図 2 は、図 1 に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明するための図である。

【0060】

まず、図 1 に示した構成において、メモ리카ード 100 内のデータ処理を管理するための鍵としては、メモ리카ードという媒体の種類に固有であり、かつ、メモ리카ードの種類等を個別に特定するための情報を含む秘密復号鍵 $K_{media}(n)$ （ n ：自然数）と、メモ리카ードごとに異なる公開暗号化鍵 $K_{Pcard}(n)$ と、公開暗号化鍵 $K_{Pcard}(n)$ により暗号化されたデータを復号するための秘密復号鍵 $K_{card}(n)$ とがある。

【0061】

ここで、鍵 $K_{card}(n)$ や鍵 $K_{Pcard}(n)$ の表記中の自然数 n は、各メモ리카ードを区別するための番号を表わす。

【0062】

すなわち、公開暗号化鍵 $K_{Pcard}(n)$ で暗号化されたデータは、各メモ리카ードごとに存在する秘密復号鍵 $K_{card}(n)$ で復号可能である。したがって、メモ리카ードにおける配信データの授受にあたっては、基本的には、後に

説明するように3つの暗号鍵 $K_{media}(n)$ 、 $K_{card}(n)$ 、 $K_{Pcard}(n)$ が用いられることになる。

【0063】

さらに、メモリカード外とメモリカード間でのデータの授受における秘密保持のための暗号鍵としては、各媒体に固有な公開暗号化鍵 $K_{Pmedia}(n)$ と、公開暗号化鍵 $K_{Pmedia}(n)$ により暗号化されたデータを復号化するための秘密復号鍵 $K_{media}(n)$ と、各通信ごと、たとえば、音楽サーバ30へのユーザのアクセスごとに音楽サーバ30、携帯電話機100または102において生成される共通鍵 K_s が用いられる。

【0064】

ここで、共通鍵 K_s は、たとえば、ユーザが音楽サーバ30に対して1回のアクセスを行なうごとに発生する構成として、1回のアクセスである限り何曲の音楽情報についても同一の共通鍵が用いられる構成としてもよいし、また、たとえば、各曲目ごとにこの共通鍵を変更したうえでその都度ユーザに配信する構成としてもよい。

【0065】

以下では、このような通信の単位あるいはアクセスの単位を「セッション」と呼ぶことにし、共通鍵 K_s を「セッションキー」とも呼ぶことにする。

【0066】

したがって、共通鍵 K_s は各通信セッションに固有の値を有することになり、配信サーバや携帯電話機において管理される。

【0067】

また、配信されるべきデータについては、まず、暗号化コンテンツデータを復号する鍵である K_c （以下、ライセンスキーと呼ぶ）があり、このライセンスキー K_c により暗号化コンテンツデータが復号化されるものとする。さらに、上述したライセンス情報として、当該コンテンツデータを特定できる管理コードや、再生を行なう回数の制限などの情報を含むライセンスIDデータ $License-ID$ 等が存在する。一方、携帯電話は、受信者を識別するためのユーザIDデータ $User-ID$ を保持している。

【 0 0 6 8 】

このような構成とすることで、ライセンス I D データに含まれる情報に応じて、著作権者側の著作権保護に関する制御を行なうことが可能であり、一方ユーザ I D データを用いることで、ユーザの個人情報の保護、たとえばユーザのアクセス履歴等が部外者から知ることができないように保護するといったような制御を行なうことが可能である。

【 0 0 6 9 】

配信データにおけるコンテンツデータ D c は、上述のとおり、たとえば音楽データであり、このコンテンツデータをライセンスキー K c で復号化可能なデータを、暗号化コンテンツデータ [D c] K c と呼ぶ。

【 0 0 7 0 】

ここで、[Y] X という表記は、データ Y を、キー（鍵）X により復号可能な暗号に変換したデータであることを示している。なお、暗号化処理、復号処理で用いられる鍵を、「キー」とも称することとする。

【 0 0 7 1 】**〔配信サーバ 1 0 の構成〕**

図 3 は、図 1 に示した配信サーバ 1 0 の構成を示す概略ブロック図である。配信サーバ 1 0 は、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンス I D 等の配信情報を保持するための配信情報データベース 3 0 4 と、各ユーザごとにコンテンツデータへのアクセス回数等に従った課金情報を保持するための課金データベース 3 0 2 と、配信情報データベース 3 0 4 および課金データベース 3 0 2 からのデータをデータバス B S 1 を介して受取り、所定の暗号化処理を行なうためのデータ処理部 3 1 0 と、通信網を介して、配信キャリア 2 0 とデータ処理部 3 1 0 との間でデータ授受を行なうための通信装置 3 5 0 とを備える。

【 0 0 7 2 】

データ処理部 3 1 0 は、データバス B S 1 上のデータに応じて、データ処理部 3 1 0 の動作を制御するための配信制御部 3 1 2 と、配信制御部 3 1 2 に制御されて、セッションキー K s を発生するためのセッションキー発生部 3 1 4 と、セ

セッションキー発生部 3 1 4 より生成されたセッションキー K_s を、公開暗号化鍵 K_{Pmedia} により暗号化して、データベース $BS1$ に与えるための暗号化処理部 3 1 6 と、各ユーザの携帯電話機においてセッションキー K_s により暗号化されたうえで送信されたデータを通信装置 3 5 0 およびデータベース $BS1$ を介して受けて、復号処理を行なう復号処理部 3 1 8 と、復号処理部 3 1 8 により抽出された公開暗号化鍵 $K_{Pcard}(n)$ を用いて、ライセンスキーやライセンス ID 等のデータを配信制御部 3 1 2 に制御されて暗号化するための暗号化処理部 3 2 0 と、暗号化処理部 3 2 0 の出力を、さらにセッションキー K_s により暗号化して、データベース $BS1$ を介して通信装置 3 5 0 に与える暗号化処理部 3 2 2 とを含む。

【0073】

〔端末（携帯電話機）の構成〕

図 4 は、図 1 に示した携帯電話機 1 0 0 の構成を説明するための概略ブロック図である。

【0074】

携帯電話機 1 0 0 は、携帯電話網により無線伝送される信号を受信するためのアンテナ 1 1 0 2 と、アンテナ 1 1 0 2 からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナ 1 1 0 2 に与えるための送受信部 1 1 0 4 と、携帯電話機 1 0 0 の各部のデータ授受を行なうためのデータベース $BS2$ と、データベース $BS2$ を介して携帯電話機 1 0 0 の動作を制御するためのコントローラ 1 1 0 6 と、受信者を識別するためのユーザ ID データ $User-ID$ を保持するユーザ ID 保持部 1 1 0 7 と、外部からの指示を携帯電話機 1 0 0 に与えるためのタッチキー部 1 1 0 8 と、コントローラ 1 1 0 6 等から出力される情報をユーザに視覚情報として与えるためのディスプレイ 1 1 1 0 と、通常の通話動作において、データベース $BS2$ を介して与えられる受信データに基づいて音声を再生するための音声再生部 1 1 1 2 と、外部との間でデータの授受を行なうためのコネクタ 1 1 2 0 と、コネクタ 1 1 2 0 からのデータをデータベース $BS2$ に与え得る信号に変換し、または、データベース $BS2$ からのデータをコネクタ 1 1 2 0 に与え得る信号に変換するための外部インターフェース

部 1 1 2 2 とを備える。

【 0 0 7 5 】

ここで、ユーザ I D データは、たとえばユーザの電話番号等のデータを含む。

携帯電話機 1 0 0 は、さらに、音楽サーバ 3 0 からのコンテンツデータを復号化処理するための着脱可能なメモリカード 1 1 0 と、メモリカード 1 1 0 とデータバス B S 2 との間のデータの授受を制御するためのメモリインタフェース 1 2 0 0 と、メモリカード 1 1 0 と携帯電話機の他の部分とのデータ授受にあたり、データバス B S 2 上においてやり取りされるデータを暗号化するためのセッションキー K s を乱数等により発生するセッションキー発生部 1 5 0 2 と、セッションキー発生部 1 5 0 2 により生成されたセッションキーを暗号化して、データバス B S 2 に与えるための暗号化処理部 1 5 0 4 と、セッションキー発生部 1 5 0 2 において生成された、データバス B S 2 上のデータをセッションキー K s により復号して出力する復号処理部 1 5 0 6 と、復号処理部 1 5 0 6 の出力を受けて、音楽信号を再生するための音楽再生部 1 5 0 8 と、音楽再生部 1 5 0 8 の出力と音声再生部 1 1 1 2 の出力とを受けて、動作モードに応じて選択的に出力するための混合部 1 5 1 0 と、混合部 1 5 1 0 の出力を受けて、外部に出力するためのアナログ信号に変換するデジタルアナログ変換部 1 5 1 2 と、デジタルアナログ変換部 1 5 1 2 の出力を受けて、ヘッドホン 1 3 0 と接続するための接続端子 1 5 1 4 とを含む。

【 0 0 7 6 】

なお、説明の簡素化のため本発明のコンテンツデータの配信に関わるブロックのみを記載し、携帯電話機が本来備えている通話機能に関するブロックについては、一部割愛されている。

【 0 0 7 7 】

[メモリカードの構成]

図 5 は、図 4 に示したメモリカード 1 1 0 の構成を説明するための概略ブロック図である。

【 0 0 7 8 】

以下では、端末 1 0 0 に装着されるメモリカード 1 1 0 の公開暗号化鍵 K P m

e d i a と、端末 1 0 2 に装着されるメモリカード 1 1 2 の公開暗号化鍵 K P m e d i a とを区別して、それぞれ、メモリカード 1 1 0 に対するものを公開暗号化鍵 K P m e d i a (1) と、メモリカード 1 1 2 に対するものを公開暗号化鍵 K P m e d i a (2) と称することにする。

【 0 0 7 9 】

また、これに対応して、公開暗号化鍵 K P m e d i a (1) で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵 K m e d i a (1) と称し、公開暗号化鍵 K P m e d i a (2) で暗号化されたデータを復号可能であって、これとは非対称な秘密復号鍵を秘密復号鍵 K m e d i a (2) と称することにする。

【 0 0 8 0 】

このように、媒体固有の公開暗号化鍵を区別することにより、以下の説明で明らかとなるように、メモリカードに複数の種類が存在する場合や、より一般的に、メモリカード以外の媒体がシステムのオプションとして存在する場合にも、対応することが可能となる。

【 0 0 8 1 】

メモリカード 1 1 0 は、メモリインタフェース 1 2 0 0 との間で信号を端子 1 2 0 2 を介して授受するデータバス B S 3 と、公開暗号化鍵 K P m e d i a (1) の値を保持し、データバス B S 3 に公開暗号化鍵 K P m e d i a (1) を出力するための K P m e d i a (1) 保持部 1 4 0 1 と、メモリカード 1 1 0 に対応する秘密復号鍵 K m e d i a (1) を保持するための K m e d i a (1) 保持部 1 4 0 2 と、データバス B S 3 にメモリインタフェース 1 2 0 0 から与えられるデータから、秘密復号鍵 K m e d i a (1) により復号処理をすることにより、セッションキー K s を抽出する復号処理部 1 4 0 4 と、公開暗号化鍵 K P c a r d (1) を保持するための K P c a r d (1) 保持部 1 4 0 5 と、復号処理部 1 4 0 4 により抽出されたセッションキー K s に基づいて、切換スイッチ 1 4 0 8 からの出力を暗号化してデータバス B S 3 に与えるための暗号化処理部 1 4 0 6 と、データバス B S 3 上のデータを復号処理部 1 4 0 4 により抽出されたセッションキー K s により復号処理してデータバス B S 4 に与えるための復号処理部 1

4 1 0 と、データバス B S 4 からメモリカードごとに異なる公開暗号化鍵 K P c a r d (n) で暗号化されているライセンスキー K c 、ライセンス I D 等のデータを格納し、データバス B S 3 からライセンスキー K c により暗号化されている暗号化コンテンツデータ [D c] K c を受けて格納するためのメモリ 1 4 1 2 とを備える。

【 0 0 8 2 】

切換えスイッチ 1 4 0 8 は、接点 P a 、 P b 、 P c を有し、接点 P a には K P c a r d (1) 保持部 1 4 0 5 からの公開暗号化鍵 K P c a r d (1) が、接点 P b にはデータバス B S 5 が、接点 P c には暗号化処理部 1 4 1 4 の出力が与えられる。切換えスイッチ 1 4 0 8 は、それぞれ、接点 P a 、 P b 、 P c に与えられる信号を、動作モードが、「配信モード」、「再生モード」、「移動モード」のいずれであるかに応じて、選択的に暗号化処理部 1 4 0 6 に与える。

【 0 0 8 3 】

メモリカード 1 1 0 は、さらに、秘密復号鍵 K c a r d (1) の値を保持するための K c a r d (1) 保持部 1 4 1 5 と、公開暗号化鍵 K P c a r d (1) により暗号化されており、かつ、メモリ 1 4 1 2 から読み出されたライセンスキー K c 、ライセンス I D 等 ([K c , L i c e n s e] K c a r d (1)) を、復号処理してデータバス B S 5 に与える復号処理部 1 4 1 6 と、データの移動処理等において、相手先のメモリカードの公開暗号化鍵 K P c a r d (n) を復号処理部 1 4 1 0 から受けて、この相手方の公開暗号化鍵 K P c a r d (n) に基づいて、データバス B S 5 上に出力されているライセンスキー K c 、ライセンス I D 等を暗号化したうえで、切換えスイッチ 1 4 0 8 に出力するための暗号化処理部 1 4 1 4 と、データバス B S 3 を介して外部とデータの授受を行い、データバス B S 5 との間でライセンス I D データ等を受けて、メモリカード 1 1 0 の動作を制御するためのコントローラ 1 4 2 0 と、データバス B S 5 との間でライセンス I D データ等のデータの授受が可能なレジスタ 1 5 0 0 とを備える。

【 0 0 8 4 】

なお、図 5 において実線で囲んだ領域は、メモリカード 1 1 0 内において、外部からの不当な開封処理等が行なわれると、内部データの消去や内部回路の破壊

により、第三者に対してその領域内に存在する回路内のデータ等の読み出しを不能化するためのモジュール T R M に組込まれているものとする。

【 0 0 8 5 】

このようなモジュールは、一般にはタンパーレジスタンスモジュール (Tamper Resistance Module) と呼ばれる。

【 0 0 8 6 】

もちろん、メモリ 1 4 1 2 も含めて、モジュール T R M 内に組み込まれる構成としてもよい。しかしながら、図 5 に示したような構成とすることで、メモリ 1 4 1 2 中に保持されているデータは、いずれも暗号化されているデータであるため、第三者はこのメモリ 1 4 1 2 中のデータのみでは、音楽を再生することは不可能であり、かつ高価なタンパーレジスタンスモジュール内にメモリ 1 4 1 2 を設ける必要がないので、製造コストが低減されるという利点がある。

【 0 0 8 7 】

図 6 および図 7 は、図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信動作を説明するための第 1 および第 2 のフローチャートである。

【 0 0 8 8 】

図 6 および図 7 においては、ユーザ 1 が、メモリカード 1 1 0 を用いることで、音楽サーバ 3 0 から音楽データの配信を受ける場合の動作を説明している。

【 0 0 8 9 】

まず、ユーザ 1 の携帯電話機 1 0 0 から、ユーザによりタッチキー 1 1 0 8 のキーボタンの操作等によって、配信リクエストがなされる (ステップ S 1 0 0)

。

【 0 0 9 0 】

メモリカード 1 1 0 においては、この配信リクエストに応じて、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化鍵 K P m e d i a (1) を音楽サーバ 3 0 に対して送信する (ステップ S 1 0 2) 。

【 0 0 9 1 】

音楽サーバ 3 0 では、メモリカード 1 1 0 から転送された配信リクエストならびに公開暗号化鍵 K P m e d i a (1) を受信すると (ステップ S 1 0 4) 、受

信した公開暗号化鍵 $KPmedia(1)$ に基づいて、認証サーバ 12 に対して照会を行ない、正規メモリカードからのアクセスの場合は次の処理に移行し（ステップ S106）、正規メモリカードでない場合には、処理を終了する（ステップ S154）。

【0092】

照会の結果、正規メモリカードであることが確認されると、音楽サーバ 30 では、セッションキー発生部 314 が、セッションキー Ks を生成する。さらに、音楽サーバ 30 内の暗号化処理部 316 が、受信した公開暗号化鍵 $KPmedia(1)$ により、このセッションキー Ks を暗号化して暗号化セッションキー $[Ks]Kmedia(1)$ を生成する（ステップ S108）。

【0093】

続いて、音楽サーバ 30 は、暗号化セッションキー $[Ks]Kmedia(1)$ をデータベース BS1 に与える。通信装置 350 は、暗号化処理部 316 からの暗号化セッションキー $[Ks]Kmedia(1)$ を、通信網を通じて、携帯電話機 100 のメモリカード 110 に対して送信する（ステップ S110）。

【0094】

携帯電話機 100 が、暗号化セッションキー $[Ks]Kmedia(1)$ を受信すると（ステップ S112）、メモリカード 110 においては、メモリインタフェース 1200 を介して、データベース BS3 に与えられた受信データを、復号処理部 1404 が、秘密復号鍵 $Kmedia(1)$ により復号処理することにより、セッションキー Ks を復号し抽出する（ステップ S114）。

【0095】

続いて、配信動作においては、切換スイッチ 1408 は、接点 Pa が閉じる状態が選択されているので、暗号化処理部 1406 は、接点 Pa を介して $KPcard(1)$ 保持部 1405 から与えられる公開暗号化鍵 $KPcard(1)$ （メモリカード 110 に対する公開暗号化鍵）を、セッションキー Ks により暗号化し（ステップ S116）、データ $[KPcard(1)]Ks$ を生成する（ステップ S118）。

【0096】

携帯電話機 1 0 0 は、暗号化処理部 1 4 0 6 により暗号化されたデータ [K P c a r d (1)] K s を音楽サーバ 3 0 に対して送信する (ステップ S 1 2 0)。

【0 0 9 7】

音楽サーバ 3 0 では、通信装置 3 5 0 によりデータ [K P c a r d (1)] K s が受信され (ステップ S 1 2 2)、データバス B S 1 に与えられたデータ [K P c a r d (1)] K s を復号処理部 3 1 8 が、セッションキー K s により復号処理して、公開暗号化鍵 K P c a r d (1) を復号抽出する (ステップ S 1 2 4)。

【0 0 9 8】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する (ステップ S 1 2 6)。

【0 0 9 9】

さらに、音楽サーバ 3 0 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、通信装置 3 5 0 を介して、メモリカード 1 1 0 に送信する (ステップ S 1 2 8)。

【0 1 0 0】

携帯電話機 1 0 0 がデータ [D c] K c を受信すると (ステップ S 1 3 0)、メモリカード 1 1 0 においては、受信したデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する (ステップ S 1 3 2)。

【0 1 0 1】

一方、音楽サーバ 3 0 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し (ステップ S 1 3 4)、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのライセンスキー K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられた公開暗号化鍵 K P c a r d (1) により暗号化処理する (ステップ S 1 3 6)。

【0 1 0 2】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c

、License] Kcard (1) を受取って、さらにセッションキーKsにより暗号化したデータをデータバスBS1に与える。通信装置350は、暗号化処理部322により暗号化されたデータ [[Kc, License] Kcard (1)] Ksをメモ리카ード110に対して送信する。

【0103】

携帯電話機100がデータ [[Kc, License] Kcard (1)] Ksを受信すると（ステップS142）、メモ리카ード110においては、復号処理部1410がセッションキーKsにより復号処理を行ない、データ [Kc, License] Kcard (1) を抽出し、メモリ1412に記録（格納）する（ステップS146）。

【0104】

さらに、メモ리카ード110においては、コントローラ1420により制御されて、復号処理部1416が、メモリ1412に格納されたデータ [Kc, License] Kcard (1) を復号し、復号されたライセンス情報データLicenseを、レジスタ1500に格納する（ステップ148）。

【0105】

以上のような動作により、メモ리카ード自身が、セッションキーKsを送る側（音楽サーバ30）に、公開暗号化鍵KPmedia (1) を送信した上で、配信を受けることができ、メモ리카ード110が格納するコンテンツデータは再生可能な状態となる。以下では、メモ리카ードが格納するコンテンツデータが再生可能な状態となっていることを、「メモ리카ード110は、状態SAにある」と呼ぶことにする。一方、メモ리카ードが格納するコンテンツデータが再生不可能な状態となっていることを、「メモ리카ード110は、状態SBにある」と呼ぶことにする。

【0106】

さらに、メモ리카ード110から音楽サーバ30へは、配信受理が通知され、音楽サーバ30で配信受理を受信すると（ステップS150）、課金データベース302にユーザ1の課金データが格納され（ステップS152）、処理が終了する（ステップS154）。

【0107】

図8は、携帯電話機100内において、メモリカード110に保持された暗号化コンテンツデータから、コンテンツデータを復号化し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【0108】

図8を参照して、携帯電話機100のタッチキー部1108等からのユーザ1の指示により、再生リクエストがメモリカード110に対して出力される（ステップS200）。

【0109】

メモリカード110においては、この再生リクエストに応じて、コントローラ1420は、レジスタ1500に保持されるライセンス情報データLicenseに基づいて、再生可能なデータに対するリクエストであるかを判断し（ステップS202）、再生可能と判断した場合は、K P m e d i a (1) 保持部1401から、公開暗号化鍵K P m e d i a (1) を携帯電話機100に対して送信する（ステップS204）。一方、再生不可能と判断した場合は、処理を終了する（ステップS230）。

【0110】

再生可能と判断され、メモリカード110から公開暗号化鍵K P m e d i a (1) が送信された場合、携帯電話機100では、メモリカード110からの公開暗号化鍵K P m e d i a (1) を受信すると（ステップS206）、K s 発生部1502においてセッションキーK s を生成し、暗号化処理部1504が、公開暗号化鍵K P m e d i a (1) により、セッションキーK s を暗号化して暗号化セッションキー[K s] K P m e d i a (1) を生成し、データバスBS2を介して、メモリカード110に対して送信する（ステップS208）。

【0111】

メモリカード110は、データバスBS2を介して、携帯電話機100により生成され、かつ暗号化されたセッションキーK s を受け取り、秘密復号鍵K m e d i a (1) により復号し、セッションキーK s を抽出する（ステップS210）。

【0 1 1 2】

続いて、メモリカード 1 1 0 は、メモリ 1 4 1 2 から、暗号化されているデータ [K c, L i c e n s e] K c a r d (1) を読み出し、復号処理部 1 4 1 6 が復号処理を行なう（ステップ S 2 1 2）。

【0 1 1 3】

秘密復号鍵 K c a r d (1) により、メモリ 1 4 1 2 から読み出されたデータを復号可能な場合（ステップ S 2 1 4）、ライセンスキー K c が抽出される（ステップ S 2 1 6）。一方、再生不可能の場合、処理は終了する（ステップ S 2 3 2）。

【0 1 1 4】

メモリ 1 4 1 2 から読み出されたデータを再生可能な場合（ステップ S 2 1 4）は、レジスタ 1 5 0 0 内のライセンス情報データ L i c e n s e のうち、再生回数に関するデータが変更される（ステップ S 2 1 8）。

【0 1 1 5】

続いて、抽出したセッションキー K s により、ライセンスキー K c を暗号化し（ステップ S 2 2 0）、暗号化されたライセンスキー [K c] K s をデータバス B S 2 に与える（ステップ S 2 2 2）。

【0 1 1 6】

携帯電話機 1 0 0 の復号処理部 1 5 0 6 は、セッションキー K s により復号化処理を行なうことにより、ライセンスキー K c を取得する（ステップ S 2 2 4）。

【0 1 1 7】

続いて、メモリカード 1 1 0 は、暗号化コンテンツデータ [D c] K c をメモリ 1 4 1 2 から読み出し、データバス B S 2 に与える（ステップ S 2 2 6）。

【0 1 1 8】

携帯電話機 1 0 0 の音楽再生部 1 5 0 8 は、暗号化コンテンツデータ [D c] K c を、抽出されたライセンスキー K c により復号処理して平文の音楽データを生成し（ステップ S 2 2 8）、音楽信号を再生して混合部 1 5 1 0 に与える（ステップ S 2 3 0）。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からの

データを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップ S 2 3 2）。

【0 1 1 9】

このような構成とすることで、メモリカード自身が、セッションキー K s を送る側（携帯電話機 1 0 0）に、公開暗号化鍵 K P m e d i a （1）を送信した上で、再生動作を行なうことが可能となる。

【0 1 2 0】

図 9 および図 1 0 は、2 つのメモリカード間において、音楽データおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 および第 2 のフローチャートである。

【0 1 2 1】

まず、携帯電話機 1 0 2 が送信側であり、携帯電話機 1 0 0 が受信側であるものとする。また、携帯電話機 1 0 2 にも、メモリカード 1 1 0 と同様の構成を有するメモリカード 1 1 2 が装着されているものとする。

【0 1 2 2】

携帯電話機 1 0 2 は、まず、自身の側のメモリカード 1 1 2 および携帯電話機 1 0 0 に対して、移動リクエストまたは複製リクエストを出力する（ステップ S 3 0 0）。

【0 1 2 3】

メモリカード 1 1 2 は、これに応じて、メモリ 1 4 1 2 内の暗号化コンテンツデータ [D c] K c を読み出して、メモリカード 1 1 0 に対して出力し（ステップ S 3 0 2）、一方、携帯電話機 1 0 0 は、携帯電話機 1 0 2 からリクエストを受信して（ステップ S 3 0 1）、メモリカード 1 1 0 では、暗号化コンテンツデータ [D c] K c をメモリ 1 4 1 2 に格納する（ステップ S 3 0 4）。

【0 1 2 4】

続いて、携帯電話機 1 0 2 および 1 0 0 においては、ステップ S 3 0 0 において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップ S 3 0 6、ステップ S 3 0 6' ）、「移動リクエスト」である場合、メモリカード 1 1 2 は、公開暗号化鍵 K P m e d i a （2）を

携帯電話機 1 0 2 に対して送信し（ステップ S 3 0 8）、携帯電話機 1 0 2 は、公開暗号化鍵 K P m e d i a (2) を受信する（ステップ S 3 1 2）。一方、メモリカード 1 1 0 は、「移動リクエスト」である場合、公開暗号化鍵 K P m e d i a (1) を携帯電話機 1 0 0 に出力し（ステップ S 3 0 8'）、携帯電話機 1 0 0 は、公開暗号化鍵 K P m e d i a (1) を携帯電話機 1 0 2 に対して送信する（ステップ S 3 1 0）。

【 0 1 2 5 】

携帯電話機 1 0 2 が、公開暗号化鍵 K P m e d i a (1) および公開暗号化鍵 K P m e d i a (2) を受信すると（ステップ S 3 1 2、ステップ S 3 1 2'）、携帯電話機 1 0 2 においては、セッションキー発生回路 1 5 0 2 は、セッションキー K s を生成し（ステップ S 3 0 3）、公開暗号化鍵 K P m e d i a (1) および公開暗号化鍵 K P m e d i a (2) を用いて、暗号化処理部 1 5 0 4 がセッションキー K s を暗号化する（ステップ S 3 1 4）。

【 0 1 2 6 】

携帯電話機 1 0 2 は、データバス B S 2 を介して、メモリカード 1 1 2 に対しては暗号化セッションキー [K s] K P m e d i a (2) を伝達し、メモリカード 1 1 2 においては、秘密復号鍵 K m e d i a (2) によりセッションキー K s を復号抽出する（ステップ S 3 2 8）。

【 0 1 2 7 】

さらに、携帯電話機 1 0 2 は、暗号化セッションキー [K s] K P m e d i a (1) を携帯電話機 1 0 0 に対して送信する（ステップ S 3 1 6）。携帯電話機 1 0 0 は、暗号化セッションキー [K s] K P m e d i a (1) を受信すると（ステップ S 3 1 8）、メモリカード 1 1 0 に伝達し、メモリカード 1 1 0 は、復号処理部 1 4 0 4 が復号して、セッションキー K s を受理する（ステップ S 3 2 0）。

【 0 1 2 8 】

メモリカード 1 1 0 においては、セッションキー K s によりメモリカード 1 1 0 の公開暗号化鍵 K P c a r d (1) を暗号化して（ステップ S 3 2 2）、携帯電話機 1 0 0 から携帯電話機 1 0 2 に対して暗号化されたデータ [K P c a r d

(1)] K s を送信する (ステップ S 3 2 4) 。携帯電話機 1 0 2 は、データ [K P c a r d (1)] K s を受信し (ステップ S 3 2 6) 、かつ、メモリカード 1 1 2 によるセッションキー K s の受理が完了すると (ステップ S 3 2 8) 、メモリカード 1 1 2 においては、メモリカード 1 1 0 から送信された暗号化データ [K P c a r d (1)] K s をセッションキー K s により復号化して、メモリカード 1 1 0 の公開暗号化鍵 K P c a r d (1) を復号抽出する (ステップ S 3 3 0) 。

【 0 1 2 9 】

続いて、メモリカード 1 1 2 においては、メモリ 1 4 1 2 からメモリカード 1 1 2 の公開暗号化鍵 K P c a r d (2) により暗号化されているライセンスキー K c 、ライセンス情報データ L i c e n s e が読み出される (ステップ S 3 3 2) 。

【 0 1 3 0 】

続いて、メモリカード 1 1 2 の復号処理部 1 4 1 6 が、秘密復号鍵 K c a r d (2) により、ライセンスキー K c 、ライセンス情報データ L i c e n s e を復号処理する (ステップ S 3 3 4) 。

【 0 1 3 1 】

メモリカード 1 1 2 のコントローラ 1 4 2 0 は、このようにして復号されたライセンス情報データ L i c e n s e の値を、レジスタ 1 5 0 0 内のデータ値と置換する (ステップ S 3 3 6) 。

【 0 1 3 2 】

さらに、メモリカード 1 1 2 の暗号化処理部 1 4 1 4 は、復号処理部 1 4 1 0 において抽出されたメモリカード 1 1 0 における公開暗号化鍵 K P c a r d (1) により、ライセンスキー K c 、ライセンス情報データ L i c e n s e とを暗号化する (ステップ S 3 3 8) 。

【 0 1 3 3 】

メモリカード 1 1 2 の暗号化処理部 1 4 1 4 により暗号化されたデータは、切換スイッチ 1 4 0 8 (接点 P c が閉じている) を介して、さらに、暗号化処理部 1 4 0 6 に与えられ、暗号化処理部 1 4 0 6 は、データ [K c , L i c e n s e

] K c a r d (1) をセッションキー K s により暗号化してデータ [[K c , L i c e n s e] K c a r d (1)] K s を生成する (ステップ S 3 4 0) 。

【 0 1 3 4 】

続いて、メモリカード 1 1 2 は、携帯電話機 1 0 2 に対してデータ [[K c , L i c e n s e] K c a r d (1)] K s を出力し (ステップ S 3 4 2) 、携帯電話機 1 0 2 はデータ [[K c , L i c e n s e] K c a r d (1)] K s を携帯電話機 1 0 0 に対して送信する (ステップ S 3 4 4) 。

【 0 1 3 5 】

携帯電話機 1 0 0 が受信したデータ [[K c , L i c e n s e] K c a r d (1)] K s は (ステップ S 3 4 6) 、メモリカード 1 1 0 に対して伝達され、メモリカード 1 1 0 の復号処理部 1 4 1 0 は、暗号化されたデータ [[K c , L i c e n s e] K c a r d (1)] K s を復号して、データ [K c , L i c e n s e] K c a r d (1) を受理する (ステップ S 3 4 8) 。

【 0 1 3 6 】

メモリカード 1 1 0 においては、復号処理部 1 4 1 0 により、セッションキー K s に基づいて復号化処理されたデータをメモリ 1 4 1 2 に記録する (ステップ S 3 5 0) 。さらに、メモリカード 1 1 0 においては、復号処理部 1 4 1 6 が、秘密復号鍵 K c a r d (1) に基づいて、データ [K c , L i c e n s e] K c a r d (1) を復号し、復号されたライセンス情報データ L i c e n s e をレジスタ 1 5 0 0 に格納する (ステップ S 3 5 2) 。

【 0 1 3 7 】

復号されたライセンス情報データ L i c e n s e のレジスタ 1 5 0 0 への格納が終了すると、メモリカード 1 1 0 は携帯電話機 1 0 0 に移動受理を通知し、携帯電話機 1 0 0 は、携帯電話機 1 0 2 に対して移動受理を送信する (ステップ S 3 5 4) 。

【 0 1 3 8 】

携帯電話機 1 0 2 は、携帯電話機 1 0 0 からの移動受理を受信すると、メモリカード 1 1 2 に対してこれを転送し、メモリカード 1 1 2 は、これに応じて、レジスタ 1 5 0 0 に格納されたライセンス情報データ L i c e n s e を消去する (

ステップ 3 5 8)。

【0 1 3 9】

一方、携帯電話機 1 0 2 では、移動受理が受信されたことに応じて、ディスプレイ 1 1 1 0 上に、ユーザ 2 に対して、メモリカード 1 1 2 のメモリ 1 4 1 2 内に格納されている移動データに対応する記憶データの消去を行なって良いかを問うメッセージを表示する。これに応じて、ユーザ 2 は、タッチキー 1 1 0 8 からこのメッセージに対する回答を入力する（ステップ S 3 6 0）。

【0 1 4 0】

レジスタ 1 5 0 0 内のデータの消去が完了し（ステップ S 3 5 8）、かつ、上記メッセージに対する回答の入力が行なわれると（ステップ S 3 6 0）、メモリカード 1 1 2 内のコントローラ 1 4 2 0 は、メモリ 1 4 1 2 内のデータの消去を行なうかの判断を行なう（ステップ S 3 6 2）。

【0 1 4 1】

メモリ 1 4 1 2 内の該当データの消去が指示されている場合（ステップ S 3 6 2）、コントローラ 1 4 2 0 により制御されて、メモリ 1 4 1 2 内の暗号化コンテンツデータ [D c] K c およびデータ [K c, L i c e n s e] K c a r d (2) が消去され（ステップ S 3 6 4）、処理が終了する（ステップ S 3 7 4）。

【0 1 4 2】

一方、メモリ 1 4 1 2 内の該当データの消去が指示されていない場合（ステップ S 3 6 2）、処理は終了する（ステップ S 3 7 4）。この場合、メモリ 1 4 1 2 内には、暗号化コンテンツデータ [D c] K c およびデータ [K c, L i c e n s e] K c a r d (2) が残っていることになるが、レジスタ 1 5 0 0 内にライセンス情報データ L i c e n s e が存在しないため、ユーザ 2 は、再度、音楽サーバ 3 0 から再生情報を配信してもらわない限り、音楽データの再生を行なうことはできない。すなわち、メモリカード 1 1 2 は「状態 S B」となる。メモリカード 1 1 0 においては、暗号化コンテンツデータ以外にも、ライセンスキー K c、ライセンス情報データが移動されているので、メモリカード 1 1 0 は「状態 S A」となっている。

【0 1 4 3】

一方、ステップ S 3 0 6 ' において、「複製リクエスト」が与えられていると判断された場合は、携帯電話機 1 0 0 から携帯電話機 1 0 2 に対して複製受取が送信される（ステップ S 3 7 0）。携帯電話機 1 0 2 において、複製受取を受信すると（ステップ S 3 7 2）、処理が終了する（ステップ S 3 7 4）。

【0 1 4 4】

このような構成とすることで、メモリカード自身が、セッションキー K s を送る側（携帯電話機 1 0 0）に、公開暗号化鍵 K P m e d i a （1）および K P m e d i a （2）を送信した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

【0 1 4 5】

〔実施の形態 2〕

実施の形態 2 のデータ配信システムにおいては、実施の形態 1 のデータ配信システムの構成と異なって、配信サーバ、携帯電話機およびメモリカードの各々が、独自のセッションキーを生成する構成となっていることを 1 つの特徴とする。すなわち、配信サーバまたは携帯電話機の発生するセッションキーをセッションキー K s とし、一方のメモリカード 1 2 0 の発生するセッションキーをセッションキー K s 1 とし、メモリカード 1 2 0 と同様の構成を有する他方のメモリカード 1 2 2 の発生するセッションキーをセッションキー K s 2 とする。

【0 1 4 6】

すなわち、実施の形態 2 のデータ配信システムにおいては、システムを構成する機器の各々が、自身でセッションキーを生成し、データを受け取るとき、言い換えるとデータの送信先になっている場合には、相手方（送信元）に対して、まず、セッションキーを配送する。送信元は、この送信先から配送されたセッションキーでデータを暗号化し、この暗号化データを送信する。送信先では、自身で生成したセッションキーにより、受け取ったデータを復号化するという構成を 1 つの特徴とするものである。

【0 1 4 7】

また、上記のような動作を実現するために、再生動作において、携帯電話機側がメモリカードの生成するセッションキーを受け取るための公開暗号化鍵を K P

pとし、この公開暗号化鍵 $K P p$ で暗号化されたデータを復号化できる秘密復号鍵を鍵 $K p$ とする。

【0 1 4 8】

図 1 1 は、実施の形態 2 のメモリカード 1 2 0 に対応した配信サーバ 1 1 の構成を示す概略ブロック図である。図 3 に示した配信サーバ 1 0 の構成と異なる点は、データ処理部 3 1 0 における暗号化処理部 3 2 2 は、 $K s$ 発生部 3 1 4 からセッションキー $K s$ に基づいてではなく、携帯電話機に装着されたメモリカードからセッションキー $K s 1$ 、 $K s 2$ により暗号化されて送信され、復号処理部 3 1 8 により復号抽出されたセッションキー、たとえば、セッションキー $K s 1$ に基づいて、暗号化処理部 3 2 0 の出力をさらに暗号化して、データバス $B S 1$ を介して通信装置 3 5 0 に与える点である。

【0 1 4 9】

配信サーバ 1 1 のその他の点は、図 3 に示した実施の形態 1 の配信サーバ 1 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 1 5 0】

図 1 2 は、実施の形態 2 における携帯電話機 1 0 1 の構成を説明するための概略ブロック図である。

【0 1 5 1】

図 4 に示した携帯電話機 1 0 0 の構成と異なる点は、まず、メモリカード 1 2 0 が装着されていること以外に、携帯電話機 1 0 1 は、公開暗号化鍵 $K P p$ を保持して、再生動作時に公開暗号化鍵 $K P p$ をデータバス $B S 2$ に出力する $K P p$ 保持部 1 5 2 4 を備える構成となっていることである。

【0 1 5 2】

さらに、携帯電話機 1 0 1 は、秘密復号鍵 $K p$ を保持する $K p$ 保持部 1 5 2 0 と、この $K p$ 保持部 1 5 2 0 から与えられる秘密復号鍵 $K p$ に基づいて、データバス $B S 2$ を介してメモリカード 1 2 0 から与えられる公開暗号化鍵 $K P p$ で暗号化されたセッションキー $K s 1$ を復号し抽出する復号処理部 1 5 2 2 とをさらに備える構成となっている。しかも、暗号化処理部 1 5 0 4 は、この復号処理部

1 5 2 2 から与えられるセッションキー K s 1 により、K s 発生部 1 5 0 2 からの自身のセッションキー K s を暗号化してデータバス B S 2 に出力する。

【0 1 5 3】

携帯電話機 1 0 1 のその他の点は、図 4 に示した実施の形態 1 の携帯電話機 1 0 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 1 5 4】

図 1 3 は、本発明の実施の形態 2 のメモリカード 1 2 0 の構成を説明するための概略ブロック図であり、実施の形態 1 の図 5 と対比される図である。

【0 1 5 5】

メモリカード 1 2 0 の構成が、メモリカード 1 1 0 の構成と異なる点は、まず、メモリカード 1 2 0 は、このカード独自のセッションキー K s 1 を発生するセッションキー K s 1 発生部 1 4 3 2 を備えることである。

【0 1 5 6】

さらに、メモリカード 1 2 0 は、セッションキー発生回路 1 4 3 2 で生成されたセッションキー K s 1 を、暗号化してデータバス B S 3 に与えるための暗号化処理部 1 4 3 0 を備える。

【0 1 5 7】

これに応じて、メモリカード 1 2 0 は、さらに、再生モードにおいて、形態電話機 1 0 1 の公開暗号化鍵 K P p を受けて保持する K P p 受理部 1 4 0 7 と、移動モードにおいて、相手方（移動先）の公開暗号化鍵 K P m e d i a (n) を受けて保持する K P m e d i a 受理部 1 4 0 3 と、この K P m e d i a 受理部 1 4 0 3 の出力と K P p 受理部 1 4 0 7 の出力とを受けて、動作モードに応じていずれか一方を出力する切換えスイッチ 1 4 3 6 を備える。切換えスイッチ 1 4 3 6 は、接点 P i および P h とを有し、接点 P i は K P p 受理部 1 4 0 7 と、接点 P h は K P m e d i a 受理部 1 4 0 3 とそれぞれ結合する。暗号化処理部 1 4 3 0 は、切換えスイッチ 1 4 3 6 から与えられる公開暗号化鍵 K P m e d i a (n) または公開暗号化鍵 K P p のいずれかにより、K s 1 発生部 1 4 3 2 からのセッションキー K s 1 を暗号化して、データバス B S 3 に与える。

【0 1 5 8】

すなわち、切換えスイッチ 1 4 3 6 は、配信動作のとき、および移動動作において移動先となっているときは、未使用状態であり、再生動作の時は、接点 P i の側に閉じており、移動動作において移動元となっているときは、接点 P h の側に閉じている。

【0 1 5 9】

メモリカード 1 2 0 は、さらに、接点 P e、P f および P g を有し、復号処理部 1 4 0 4 から与えられる音楽サーバからのセッションキー K s と、K s 1 発生部 1 4 3 2 の出力と、データバス B S 4 から与えられる携帯電話機 1 0 1 からのセッションキー K s とを受けて、動作モードに応じていずれか 1 つを選択的に出力する切換えスイッチ 1 4 3 5 を備える。接点 P e には復号処理部 1 4 0 4 からの出力が、接点 P f には K s 1 発生部 1 4 3 2 の出力が、接点 P g にはデータバス B S 4 がそれぞれ結合している。したがって、暗号化処理部 1 4 0 6 と復号処理部 1 4 1 0 は、この切換えスイッチ 1 4 3 5 から与えられるキーに基づいて、それぞれ、暗号化処理および復号処理を行なう。

【0 1 6 0】

すなわち、切換えスイッチ 1 4 3 5 は、配信動作の場合に音楽サーバ 3 1 からのセッションキー K s 1 の抽出を行なうときは、接点 P e の側に閉じており、配信動作の場合に音楽サーバ 3 1 からの暗号化されたライセンスキー K c、ライセンス情報データについてセッションキー K s 1 による復号を行なうときは、接点 P f の側に閉じている。切換えスイッチ 1 4 3 5 は、再生動作において復号処理を行なうときは、接点 P f の側に閉じており、再生動作において暗号化処理を行なうときは、接点 P g の側に閉じている。切換えスイッチ 1 4 3 5 は、移動動作において移動元となっている場合に復号処理を行なうときは、接点 P f の側に閉じており、移動動作において移動元となっている場合に暗号化処理を行なうときは、接点 P g の側に閉じている。切換えスイッチ 1 4 3 5 は、移動動作において移動先となっている場合に移動元のセッションキーを受け取るときは、接点 P e の側に閉じており、移動動作において移動先となっている場合にライセンスキー K c およびライセンス情報データ L i c e n s e を受け取るときは、接点 P f の

側に閉じている。

【0 1 6 1】

メモリカード 1 2 0 は、さらに、接点 P a、P b、P c および P d を有し、K s 1 発生部 1 4 3 2 から与えられる自身のセッションキー K s 1 と、K P c a r d 保持部 1 4 0 5 の出力と、データバス B S 5 から与えられるライセンスキー K c と、暗号化処理部 1 4 1 4 から与えられ、相手方の公開暗号化鍵 K P c a r d (n) により暗号化されたライセンスキー K c およびライセンス情報データ L i c e n s e を受けて、動作モードに応じていずれか 1 つを選択的に出力する切換えスイッチ 1 4 0 9 を、切換えスイッチ 1 4 0 8 の替わりに備える。

【0 1 6 2】

接点 P a には K s 1 発生部 1 4 3 2 からの出力が、接点 P b には K P c a r d (1) 保持部 1 4 0 5 の出力が、接点 P c にはデータバス B S 5 が、接点 P d には暗号化処理部 1 4 1 4 の出力が、それぞれ結合している。したがって、暗号化処理部 1 4 0 6 は、この切換えスイッチ 1 4 0 9 から与えられるデータに対して、それぞれ、暗号化処理を行なう。

【0 1 6 3】

すなわち、切換えスイッチ 1 4 0 9 は、配信モードにおいて、配信先となっている場合に音楽サーバ 3 1 に自身の公開暗号化鍵 K P c a r d (1) や自身のセッションキー K s 1 を送信するときは、順次、接点 P b の側および接点 P a の側に閉じる。切換えスイッチ 1 4 0 9 は、再生モードのときは、接点 P c の側に閉じており、移動モードにおいて移動元となっているときは、接点 P d の側に閉じている。切換えスイッチ 1 4 0 9 は、移動モードにおいて移動先となっている場合にも移動元に自身の公開暗号化鍵 K P c a r d (1) や自身のセッションキー K s 1 を送信するときは、順次、接点 P b の側および接点 P a の側に閉じる。

【0 1 6 4】

図 1 4 および図 1 5 は、図 1 3 で説明したメモリカード 1 2 0 を用いた配信モードを説明するための第 1 および第 2 のフローチャートである。

【0 1 6 5】

図 1 4 および図 1 5 においても、ユーザ 1 が、メモリカード 1 2 0 を用いるこ

とで、音楽サーバ 3 1 から音楽データの配信を受ける配信モードの動作を説明している。

【0 1 6 6】

まず、ユーザ 1 の携帯電話機 1 0 1 から、ユーザによりタッチキー 1 1 0 8 のキーボタンの操作等によって、配信リクエストがなされる（ステップ S 1 0 0）。

【0 1 6 7】

メモリカード 1 2 0 においては、この配信リクエストに応じて、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化鍵 K P m e d i a (1) を音楽サーバ 3 1 に対して送信する（ステップ S 1 0 2）。さらに、メモリカード 1 2 0 においては、K s 1 発生部 1 4 3 2 によりセッションキー K s 1 が生成される（ステップ S 1 0 9）。

【0 1 6 8】

音楽サーバ 3 1 では、メモリカード 1 2 0 から転送された配信リクエストならびに公開暗号化鍵 K P m e d i a (1) を受信すると（ステップ S 1 0 4）、受信した公開暗号化鍵 K P m e d i a (1) に基づいて、認証サーバ 1 2 に対して照会を行ない、正規のメモリカードを用いたアクセスの場合は次の処理に移行し（ステップ S 1 0 6）、正規のメモリカードでない場合には、処理を終了する（ステップ S 1 5 4）。

【0 1 6 9】

照会の結果、正規のメモリカードであることが確認されると、音楽サーバ 3 1 では、セッションキー発生部 3 1 4 が、セッションキー K s を生成する。さらに、音楽サーバ 3 1 内の暗号化処理部 3 1 6 が、受信した公開暗号化鍵 K P m e d i a (1) により、このセッションキー K s を暗号化して暗号化セッションキー [K s] K m e d i a (1) を生成する（ステップ S 1 0 8）。

【0 1 7 0】

続いて、音楽サーバ 3 1 は、暗号化セッションキー [K s] K m e d i a (1) をデータバス B S 1 に与える。通信装置 3 5 0 は、暗号化処理部 3 1 6 からの暗号化セッションキー [K s] K m e d i a (1) を、通信網を通じて、携帯電

話機 1 0 1 のメモリカード 1 2 0 に対して送信する（ステップ S 1 1 0）。

【0 1 7 1】

携帯電話機 1 0 1 が、暗号化セッションキー [K s] K m e d i a (1) を受信すると（ステップ S 1 1 2）、メモリカード 1 2 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス B S 3 に与えられた受信データを、復号処理部 1 4 0 4 が、秘密復号鍵 K m e d i a (1) で復号処理することにより、セッションキー K s を復号し抽出する（ステップ S 1 1 4）。

【0 1 7 2】

続いて、配信モードにおいては、切換えスイッチ 1 4 0 9 は、接点 P a または P b が順次閉じる状態が選択されるので、暗号化処理部 1 4 0 6 は、接点 P a を介してセッションキー発生部 1 4 3 2 から与えられるセッションキー K s 1 と接点 P b を介して K P c a r d (1) 保持部 1 4 0 5 から与えられる公開暗号化鍵 K P c a r d (1)（メモリカード 1 2 0 に対する公開暗号化鍵）とを、セッションキー K s により暗号化し（ステップ S 1 1 6）、データ [K P c a r d (1)、K s 1] K s を生成する（ステップ S 1 1 8）。

【0 1 7 3】

携帯電話機 1 0 1 は、暗号化処理部 1 4 0 6 により暗号化されたデータ [K P c a r d (1)、K s 1] K s を音楽サーバ 3 1 に対して送信する（ステップ S 1 2 0）。

【0 1 7 4】

音楽サーバ 3 1 では、通信装置 3 5 0 によりデータ [K P c a r d (1)、K s 1] K s が受信され（ステップ S 1 2 2）、データバス B S 1 に与えられたデータ [K P c a r d (1)、K s 1] K s を復号処理部 3 1 8 が、セッションキー K s により復号処理して、公開暗号化鍵 K P c a r d (1) およびセッションキー K s 1 を復号抽出する（ステップ S 1 2 4）。

【0 1 7 5】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する（ステップ S 1 2 6）。

【0 1 7 6】

さらに、音楽サーバ 3 1 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、通信装置 3 5 0 を介して、メモ리카ード 1 2 0 に送信する（ステップ S 1 2 8）。

【0 1 7 7】

携帯電話機 1 0 1 が暗号化コンテンツデータ [D c] K c を受信すると（ステップ S 1 3 0）、メモ리카ード 1 2 0 においては、受信した暗号化コンテンツデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する（ステップ S 1 3 2）。

【0 1 7 8】

一方、音楽サーバ 3 1 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し（ステップ S 1 3 4）、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのライセンスキー K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられた公開暗号化鍵 K P c a r d (1) により暗号化処理する（ステップ S 1 3 6）。

【0 1 7 9】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c、L i c e n s e] K c a r d (1) を受取って、さらに、メモ리카ード 1 2 0 からのセッションキー K s 1 により暗号化したデータをデータバス B S 1 に与える。通信装置 3 5 0 は、暗号化処理部 3 2 2 により暗号化されたデータ [[K c、L i c e n s e] K c a r d (1)] K s 1 をメモ리카ード 1 2 0 に対して送信する。

【0 1 8 0】

携帯電話機 1 0 1 がデータ [[K c、L i c e n s e] K c a r d (1)] K s 1 を受信すると（ステップ S 1 4 2）、メモ리카ード 1 2 0 においては、復号処理部 1 4 1 0 が接点 P f を介して K s 1 発生部 1 4 3 2 から与えられるセッションキー K s 1 により復号処理を行ない、データ [K c、L i c e n s e] K c a r d (1) を抽出し、メモリ 1 4 1 2 に格納する（ステップ S 1 4 6）。

【0 1 8 1】

さらに、メモ리카ード 1 2 0 においては、コントローラ 1 4 2 0 により制御さ

れて、復号処理部 1 4 1 6 が、メモリ 1 4 1 2 に格納されたデータ [K c , L i c e n s e] K c a r d (1) を復号し、復号されたライセンス情報データ L i c e n s e を、レジスタ 1 5 0 0 に格納する（ステップ 1 4 8 ）。

【0 1 8 2】

以上のような動作により、メモリカード 1 2 0 自身が、暗号化コンテンツデータを送る側（音楽サーバ 3 1 ）に、公開暗号化鍵 K P m e d i a (1) およびセッションキー K s 1 を送信した上で、配信を受けることができ、メモリカード 1 2 0 は、音楽情報を再生可能な状態となる。

【0 1 8 3】

さらに、メモリカード 1 2 0 から音楽サーバ 3 1 へは、配信受理が通知され、音楽サーバ 3 1 で配信受理を受信すると（ステップ S 1 5 0 ）、課金データベース 3 0 2 にユーザ 1 の課金データが格納され（ステップ S 1 5 2 ）、処理が終了する（ステップ S 1 5 4 ）。

【0 1 8 4】

図 1 6 および図 1 7 は、携帯電話機 1 0 1 内において、メモリカード 1 2 0 に保持された暗号化コンテンツデータから、音楽データであるコンテンツデータを復号化し、音楽として外部に出力するための再生モードを説明する第 1 および第 2 のフローチャートである。

【0 1 8 5】

図 1 6 および図 1 7 を参照して、携帯電話機のタッチキー 1 1 0 8 等からのユーザ 1 の指示により、再生リクエストがメモリカード 1 2 0 に対して出力される（ステップ S 2 0 0 ）。

【0 1 8 6】

メモリカード 1 2 0 においては、この再生リクエストに応じて、コントローラ 1 4 2 0 は、レジスタ 1 5 0 0 に保持されるライセンス情報データ L i c e n s e に基づいて、復号可能なデータに対するリクエストであるかを判断し（ステップ S 2 0 2 ）、再生可能と判断した場合は、再生可能通知を携帯電話機 1 0 1 に対して送信する（ステップ S 2 4 0 ）。一方、再生不可能と判断した場合は、処理を終了する（ステップ S 2 8 0 ）。

【0187】

再生可能と判断され、メモリカード120から再生可能通知が送信された場合、携帯電話機101では、公開暗号化鍵K P pをメモリカード120に送信し（ステップS242）、K s 発生部1502においてセッションキーK s を生成する（ステップS244）。

【0188】

一方、メモリカード120も、セッションキーK s 1を生成する（ステップS240）。メモリカード120は、さらに、データバスB S 2を介して携帯電話機101から受けとった公開暗号化鍵K P pによりセッションキーK s 1を暗号化し（ステップS248）、生成された暗号化セッションキー [K s 1] K pを携帯電話機101に対して送信する（ステップS250）。

【0189】

携帯電話機101では、メモリカード120からの暗号化セッションキー [K s 1] K pを受信すると、復号処理部1522が、秘密復号鍵K pにより復号化してメモリカード120で生成したセッションキーK s 1を抽出する（ステップS252）。続いて、携帯電話機101の暗号化処理部1504は、携帯電話機101で生成したセッションキーK s をセッションキーK s 1により暗号化して、暗号化セッションキー [K s] K s 1を生成し（ステップS254）、この暗号化セッションキー [K s] K s 1をメモリカード120に対して送信する（ステップS256）。

【0190】

メモリカード120は、データバスB S 2を介して、携帯電話機101により生成された暗号化セッションキー [K s] K s 1を受け取り、セッションキーK s 1により復号し、携帯電話機101で生成したセッションキーK s を抽出する（ステップS258）。

【0191】

続いて、メモリカード120は、メモリ1412から、暗号化されているデータ [K c, L i c e n s e] K c a r d (1)を読み出し、復号処理部1416が復号処理を行なう（ステップS260）。

【0192】

秘密復号鍵 K c a r d (1) により、メモリ 1 4 1 2 から読み出されたデータを復号可能な場合（ステップ S 2 6 2）、ライセンスキー K c が抽出される（ステップ S 2 6 4）。一方、復号不可能の場合、処理は終了する（ステップ S 2 8 0）。

【0193】

メモリ 1 4 1 2 から読み出されたデータを復号可能な場合は、さらに、レジスタ 1 5 0 0 内のライセンス情報データ L i c e n s e のうち、再生回数に関するデータが変更される（ステップ S 2 6 6）。

【0194】

続いて、メモ리카ード 1 2 0 においては、暗号化処理部 1 4 0 6 が、抽出したセッションキー K s により、ライセンスキー K c を暗号化し（ステップ S 2 6 8）、暗号化ライセンスキー [K c] K s をデータバス B S 2 に与える（ステップ S 2 7 0）。

【0195】

携帯電話機 1 0 1 の復号処理部 1 5 0 6 は、セッションキー K s により復号化処理を行なうことにより、ライセンスキー K c を取得する（ステップ S 2 7 2）。

【0196】

続いて、メモ리카ード 1 2 0 は、暗号化コンテンツデータ [D c] K c をメモリ 1 4 1 2 から読み出し、データバス B S 2 に与える（ステップ S 2 7 4）。

【0197】

携帯電話機 1 0 1 の音楽再生部 1 5 0 8 は、暗号化コンテンツデータ [D c] K c を、抽出されたライセンスキー K c により復号処理して平文のコンテンツデータを生成し（ステップ S 2 7 6）、音楽信号を再生して混合部 1 5 1 0 に与える（ステップ S 2 7 6）。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からの音楽信号を受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップ S 2 3 2）。

【0198】

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキー $K_s 1$ または K_s を生成し、これにより暗号化されたデータの授受を行なった上で、再生動作を行なうことが可能となる。

【0199】

図18および図19は、2つのメモリカード間において、コンテンツデータおよびキーデータ等の移動モードまたは複製モードを行なう処理を説明するための第1および第2のフローチャートである。

【0200】

まず、携帯電話機101と同様の構成を有する携帯電話機103が送信側であり、携帯電話機101が受信側であるものとする。また、携帯電話機103にも、メモリカード120と同様の構成を有するメモリカード122が装着されているものとする。

【0201】

携帯電話機103は、まず、自身の側のメモリカード122および携帯電話機101に対して、移動リクエストまたは複製リクエストを出力する（ステップS300）。

【0202】

メモリカード122は、これに応じて、メモリ1412内の暗号化コンテンツデータ $[D_c] K_c$ を読み出して、メモリカード120に対して出力し（ステップS302）、一方、携帯電話機101は、携帯電話機103からのリクエストを受信し（ステップS301）、メモリカード120では、暗号化コンテンツデータ $[D_c] K_c$ をメモリ1412に格納する（ステップS304）。

【0203】

続いて、携帯電話機103および101においては、ステップS300において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップS306、ステップS306'）、「移動リクエスト」である場合、メモリカード120は、公開暗号化鍵 $K_{Pmedia}(1)$ を携帯電話機101に出力し（ステップS308）、携帯電話機101は、公開暗号化鍵 $K_{Pmedia}(1)$ を携帯電話機103に対して送信する（ステップS

3 1 0)。

【0 2 0 4】

携帯電話機 1 0 3 が、公開暗号化鍵 $K P m e d i a (1)$ を受信し (ステップ S 3 1 2)、メモ리카ード 1 2 2 に転送すると (ステップ S 3 1 3)、メモ리카ード 1 2 2 の $K s 2$ 発生回路 1 4 3 2 は、セッションキー $K s 2$ を生成し (ステップ S 3 1 4)、公開暗号化鍵 $K P m e d i a (1)$ を用いて、暗号化処理部 1 4 3 0 がセッションキー $K s 2$ を暗号化する (ステップ S 3 1 5)。

【0 2 0 5】

携帯電話機 1 0 3 は、暗号化セッションキー $[K s 2] K P m e d i a (1)$ を携帯電話機 1 0 1 に対して送信する (ステップ S 3 1 6)。携帯電話機 1 0 1 は、暗号化セッションキー $[K s 2] K P m e d i a (1)$ を受信すると (ステップ S 3 1 8)、メモ리카ード 1 2 0 に伝達し、メモ리카ード 1 2 0 は、復号処理部 1 4 0 4 が復号して、セッションキー $K s 2$ を受理し、さらに、セッションキー生成部 1 4 3 2 で、メモ리카ード 1 2 0 におけるセッションキー $K s 1$ が生成される (ステップ S 3 2 0)。

【0 2 0 6】

メモ리카ード 1 2 0 においては、セッションキー $K s 2$ によりメモ리카ード 1 2 0 の公開暗号化鍵 $K P c a r d (1)$ およびセッションキー $K s 1$ を暗号化して (ステップ S 3 2 2)、携帯電話機 1 0 1 から携帯電話機 1 0 3 に対して暗号化されたデータ $[K P c a r d (1), K s 1] K s 2$ を送信する (ステップ S 3 2 4)。携帯電話機 1 0 3 は、データ $[K P c a r d (1), K s 1] K s 2$ を受信し (ステップ S 3 2 6)、メモ리카ード 1 2 2 に転送する。

【0 2 0 7】

メモ리카ード 1 2 2 においては、復号処理部 1 4 1 0 が、メモ리카ード 1 2 0 から送信された暗号化データ $[K P c a r d (1), K s 1] K s 2$ をセッションキー $K s 2$ により復号化して、メモ리카ード 1 2 0 の公開暗号化鍵 $K P c a r d (1)$ 、セッションキー $K s 1$ を復号抽出する (ステップ S 3 3 0)。

【0 2 0 8】

続いて、メモ리카ード 1 2 2 においては、メモリ 1 4 1 2 からメモ리카ード 1

2 2 の公開暗号化鍵 K P c a r d (2) により暗号化されているライセンスキー K c 、ライセンス情報データ L i c e n s e に対応する [K c 、 L i c e n s e] K c a r d (2) が読み出される (ステップ S 3 3 2) 。

【 0 2 0 9 】

続いて、メモ리카ード 1 2 2 の復号処理部 1 4 1 6 が、秘密復号鍵 K c a r d (2) により、[K c 、 L i c e n s e] K c a r d (2) を復号処理する (ステップ S 3 3 4) 。

【 0 2 1 0 】

メモ리카ード 1 2 2 のコントローラ 1 4 2 0 は、このようにして復号されたライセンス情報データ L i c e n s e の値を、レジスタ 1 5 0 0 内のデータ値と置換する (ステップ S 3 3 6) 。

【 0 2 1 1 】

さらに、メモ리카ード 1 2 2 の暗号化処理部 1 4 1 4 は、復号処理部 1 4 1 0 において抽出されたメモ리카ード 1 2 0 における公開暗号化鍵 K P c a r d (1) により、ライセンスキー K c 、ライセンス情報データ L i c e n s e とを暗号化する (ステップ S 3 3 8) 。

【 0 2 1 2 】

メモ리카ード 1 2 2 の暗号化処理部 1 4 1 4 により暗号化されたデータは、切換えスイッチ 1 4 0 9 (接点 P d が閉じている) を介して、さらに、暗号化処理部 1 4 0 6 に与えられ、メモ리카ード 1 2 2 の暗号化処理部 1 4 0 6 は、データ [K c , L i c e n s e] K c a r d (1) をセッションキー K s 1 により暗号化してデータ [[K c , L i c e n s e] K c a r d (1)] K s 1 を生成する (ステップ S 3 4 0) 。

【 0 2 1 3 】

続いて、メモ리카ード 1 2 2 は、携帯電話機 1 0 3 に対してデータ [[K c , L i c e n s e] K c a r d (1)] K s 1 を出力し (ステップ S 3 4 2) 、携帯電話機 1 0 3 はデータ [[K c , L i c e n s e] K c a r d (1)] K s 1 を携帯電話機 1 0 1 に対して送信する (ステップ S 3 4 4) 。

【 0 2 1 4 】

携帯電話機 1 0 1 が受信したデータ [[K c , L i c e n s e] K c a r d (1)] K s 1 は (ステップ S 3 4 6) 、メモリカード 1 2 0 に対して伝達され、メモリカード 1 2 0 の復号処理部 1 4 1 0 は、暗号化されたデータ [[K c , L i c e n s e] K c a r d (1)] K s 1 を復号して、データ [K c , L i c e n s e] K c a r d (1) を受理する (ステップ S 3 4 8) 。

【 0 2 1 5 】

メモリカード 1 2 0 においては、復号処理部 1 4 1 0 により、セッションキー K s 1 に基づいて復号化処理されたデータ [K c , L i c e n s e] K c a r d (1) をメモリ 1 4 1 2 に格納する (ステップ S 3 5 0) 。さらに、メモリカード 1 2 0 においては、復号処理部 1 4 1 6 が、秘密復号鍵 K c a r d (1) に基づいて、データ [K c , L i c e n s e] K c a r d (1) を復号し、復号されたライセンス情報データ L i c e n s e をレジスタ 1 5 0 0 に格納する (ステップ S 3 5 2) 。

【 0 2 1 6 】

以後の移動モードにおける処理ならびに複製モードにおけるメモリカード 1 2 0 および 1 2 2 の処理は、図 9 および図 1 0 で説明した実施の形態 1 のメモリカード 1 1 0 、 1 1 2 等の処理と同様であるので、その説明は繰り返さない。

【 0 2 1 7 】

このような構成とすることで、移動元および移動先のメモリカード自身が、セッションキーをそれぞれ生成した上で、移動モードを行なうが可能となる。

【 0 2 1 8 】

したがって、データバス上等で伝達されるデータのライセンスキー K c およびライセンス情報データ L i c e n s e を暗号化する鍵が、セッションごとに、かつ、機器ごとに変更されるので、ライセンスキー K c およびライセンス情報データ L i c e n s e の授受のセキュリティが一層向上するという効果がある。

【 0 2 1 9 】

しかも、以上のような構成を用いることで、たとえば、メモリカード 1 2 2 からメモリカード 1 2 0 へのデータの移動を、上述したようなセッションキー発生回路 1 5 0 2 を有する携帯電話端末を介さずに、メモリカードとメモリカードと

を接続可能なインターフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

【0 2 2 0】

ここで、移動時には、再生回数を制限するライセンス情報データ内の設定については、メモリ 1 4 1 2 に記録されたライセンス情報データを、レジスタ 1 5 0 0 にて再生の都度修正された再生回数を記録したライセンス情報データに変更することで、ライセンス情報データを更新する。このようにして、メモリカード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

【0 2 2 1】

[実施の形態 3]

実施の形態 3 のデータ配信システムにおいては、ユーザは、配信キャリアである携帯電話会社から暗号化コンテンツデータの配信を受けるのではなく、たとえば、街頭などに設置されているコンテンツデータ販売機から暗号化コンテンツデータの供給を受ける構成となっていることを 1 つの特徴とする。

【0 2 2 2】

図 2 0 は、このような実施の形態 3 のデータ配信システムの構成を説明するための概念図である。なお、携帯電話機 1 0 0 およびメモリカード 1 1 0 の構成は実施の形態 1 で説明したものと同様であるので、その説明は繰り返さない。

【0 2 2 3】

図 2 0 を参照して、コンテンツデータ販売機 2 0 0 0 は、ユーザに対して配信作業における案内等を出力するためのディスプレイ 2 0 0 2 と、ユーザから指示を入力するためのキーボード 2 0 0 4 と、料金投入口 2 0 0 6 と、携帯電話機 1 0 0 とコネクタ 1 1 2 0 を介してデータの授受を行なうための外部コネクタ 2 0 1 0 とを備える。さらに、コンテンツデータ販売機 2 0 0 0 は、携帯電話網等の通信路を介して、販売記録等を管理するための管理サーバ 2 2 0 0 と接続している。

【0 2 2 4】

図 2 1 は、実施の形態 3 のコンテンツデータ販売機 2 0 0 0 の構成を示す概略ブロック図である。コンテンツデータ販売機 2 0 0 0 は、上述したように、ディスプレイ 2 0 0 2 と、キーボード 2 0 0 4 と、料金投入口 2 0 0 6 からの投入金を受ける料金受理部 2 0 2 0 と、外部コネクタ 2 0 1 0 と、コネクタ 2 0 1 0 とデータバスとの間に設けられるインターフェース部 2 0 1 2 と、コンテンツデータ（音楽データ）を所定の方式に従って暗号化したデータや、ライセンス情報データ等の配信情報を保持するための配信情報データベース 3 0 4 と、管理サーバ 2 2 0 0 との間で情報の授受をするための通信装置 3 6 0 と、配信情報データベース 3 0 4 および管理サーバ 2 2 0 0 からのデータをデータバス B S 1 を介して受取り、所定の暗号化処理を行なうためのデータ処理部 2 1 0 0 とを備える。

【0 2 2 5】

データ処理部 2 1 0 0 中は、実施の形態 1 と同様に、データバス B S 1 上のデータに応じて、データ処理部 2 1 0 0 の動作を制御するための配信制御部 3 1 2 と、配信制御部 3 1 2 に制御されて、セッションキー K s を発生するためのセッションキー発生部 3 1 4 と、セッションキー発生部 3 1 4 より生成されたセッションキー K s を、カード媒体に固有な公開暗号化鍵 K P m e d i a (n) により暗号化して、データバス B S 1 に与えるための暗号化処理部 3 1 6 と、各ユーザの携帯電話機においてセッションキー K s により暗号化されたうえでコネクタ 2 0 1 0 から与えられたデータをデータバス B S 1 を介して受けて、復号処理を行なう復号処理部 3 1 8 と、復号処理部 3 1 8 により抽出された公開暗号化鍵 K P c a r d (n) を用いて、ライセンス情報データを配信制御部 3 1 2 に制御されて暗号化するための暗号化処理部 3 2 0 と、暗号化処理部 3 2 0 の出力を、さらにセッションキー K s により暗号化して、データバス B S 1 を介してコネクタ 2 0 1 0 に与える暗号化処理部 3 2 2 とを含む。

【0 2 2 6】

図 2 2 および図 2 3 は、図 2 0 および図 2 1 で説明したデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

【0 2 2 7】

図 2 2 および図 2 3 においては、ユーザ 1 が、メモリカード 1 1 0 を用いるこ

とで、コンテンツデータ販売機 2 0 0 0 から音楽データの配信を受ける場合の動作を説明している。

【0 2 2 8】

まず、ユーザが、コンテンツデータ販売機 2 0 0 0 のキーボード 2 0 0 4 のキーボタンの操作等によって、配信リクエストを指示する（ステップ S 4 0 0）。コンテンツデータ販売機 2 0 0 0 は、メモリカード 1 1 0 に対して公開暗号化鍵 K P m e d i a (1) の送信依頼を出力する（ステップ S 4 0 2）。

【0 2 2 9】

メモリカード 1 1 0 においては、この公開暗号化鍵 K P m e d i a (1) の送信依頼に応じて、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化鍵 K P m e d i a (1) を携帯電話機 1 0 0 に対して出力する（ステップ S 4 0 6）。

【0 2 3 0】

携帯電話機 1 0 0 がコンテンツデータ販売機 2 0 0 0 に公開暗号化鍵 K P m e d i a (1) を送信し（ステップ S 4 0 8）、コンテンツデータ販売機 2 0 0 0 が、メモリカード 1 1 0 から転送された公開暗号化鍵 K P m e d i a (1) を受信すると（ステップ S 4 1 0）、ディスプレイ 2 0 0 2 を介してユーザに料金投入を案内し、料金徴収を行なう（ステップ S 4 1 2）。続いて、コンテンツデータ販売機 2 0 0 0 は、セッションキー発生部 3 1 4 が、セッションキー K s を生成する。さらに、コンテンツデータ販売機 2 0 0 0 内の暗号化処理部 3 1 6 が、受信した公開暗号化鍵 K P m e d i a (1) により、このセッションキー K s を暗号化して暗号化セッションキー [K s] K m e d i a (1) を生成する（ステップ S 4 1 4）。

【0 2 3 1】

続いて、コンテンツデータ販売機 2 0 0 0 は、暗号化セッションキー [K s] K m e d i a (1) をデータバス B S 1 に与え、コネクタ 2 0 1 0 から出力する（ステップ S 4 1 6）。携帯電話機 1 0 0 は、この暗号化セッションキー [K s] K m e d i a (1) を受信すると、メモリカード 1 1 0 に転送する（ステップ S 4 1 8）。

【0 2 3 2】

メモリカード 1 1 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス B S 3 に与えられた暗号化セッションキー [K s] K m e d i a (1) を、復号処理部 1 4 0 4 が、秘密復号鍵 K m e d i a (1) により復号処理することにより、セッションキー K s を復号し抽出する（ステップ S 4 2 0）。

【0 2 3 3】

続いて、配信モードにおいては、切換えスイッチ 1 4 0 8 は、接点 P a が閉じる状態が選択されているので、暗号化処理部 1 4 0 6 は、接点 P a を介して K P c a r d (1) 保持部 1 4 0 5 から与えられる公開暗号化鍵 K P c a r d (1) を、セッションキー K s により暗号化し（ステップ S 4 2 2）、データ [K P c a r d (1)] K s を生成する（ステップ S 4 2 4）。

【0 2 3 4】

携帯電話機 1 0 0 は、暗号化処理部 1 4 0 6 により暗号化されたデータ [K P c a r d (1)] K s をコンテンツデータ販売機 2 0 0 0 に対して送信する（ステップ S 4 2 6）。

【0 2 3 5】

コンテンツデータ販売機 2 0 0 0 では、コネクタ 2 0 1 0 を介してデータ [K P c a r d (1)] K s が受信され（ステップ S 4 2 8）、データバス B S 1 に与えられたデータ [K P c a r d (1)] K s を復号処理部 3 1 8 が、セッションキー K s により復号処理して、公開暗号鍵 K P c a r d (1) を復号抽出する（ステップ S 4 3 0）。

【0 2 3 6】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する（ステップ S 4 3 2）。

【0 2 3 7】

さらに、コンテンツデータ販売機 2 0 0 0 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、コネクタ 2 0 1 0 を介して、携帯電話機 1 0 0 に送信する（ステップ S 4 3 4）。

【0 2 3 8】

携帯電話機 1 0 0 が暗号化コンテンツデータ [D c] K c を受信すると（ステップ S 4 3 6）、メモリカード 1 1 0 においては、受信した暗号コンテンツデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する（ステップ S 4 3 8）。

【0 2 3 9】

一方、コンテンツデータ販売機 2 0 0 0 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し（ステップ S 4 4 0）、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのライセンスキー K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられた公開暗号化鍵 K P c a r d (1) により暗号化処理する（ステップ S 4 4 2）。

【0 2 4 0】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c、L i c e n s e] K c a r d (1) を受取って、さらにセッションキー K s により暗号化したデータをデータベース B S 1 に与え、暗号化処理部 3 2 2 により暗号化されたデータ [[K c, L i c e n s e] K c a r d (1)] K s がメモリカード 1 1 0 に対して送信される（ステップ S 4 4 6）。

【0 2 4 1】

携帯電話機 1 0 0 がデータ [[K c, L i c e n s e] K c a r d (1)] K s を受信すると（ステップ S 4 4 8）、メモリカード 1 1 0 においては、復号処理部 1 4 1 0 がセッションキー K s により復号処理を行ない、データ [K c, L i c e n s e] K c a r d (1) を抽出し、メモリ 1 4 1 2 に格納する（ステップ S 4 5 2）。

【0 2 4 2】

さらに、メモリカード 1 1 0 においては、コントローラ 1 4 2 0 により制御されて、復号処理部 1 4 1 6 が、メモリ 1 4 1 2 に格納されたデータ [K c, L i c e n s e] K c a r d (1) を復号し、復号されたライセンス情報データ L i c e n s e を、レジスタ 1 5 0 0 に格納する（ステップ S 4 5 8）。

【0 2 4 3】

以上のような動作により、メモリカード自身が、セッションキー K s を送る側（コンテンツデータ販売機 2 0 0 0）に、公開暗号化鍵 K P m e d i a (1) を

送信した上で、配信を受けることができ、メモリカード 1 1 0 に格納された暗号化コンテンツデータを用いて音楽を再生可能な状態となる。

【0 2 4 4】

さらに、メモリカード 1 1 0 からコンテンツデータ販売機 2 0 0 0 へは、携帯電話機 1 0 0 を介して配信受理が通知され（ステップ S 4 6 0）、コンテンツデータ販売機 2 0 0 0 で配信受理を受信すると（ステップ S 4 6 2）、管理サーバに販売記録が送信され（ステップ S 4 6 4）、処理が終了する（ステップ S 4 6 6）。

【0 2 4 5】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等の配信を受けることができる。

【0 2 4 6】

〔実施の形態 3 の変形例〕

実施の形態 3 のデータ配信システムにおいては、メモリカード 1 1 0 は、携帯電話機 1 0 0 を介して、コンテンツデータ販売機 2 0 0 0 から暗号化コンテンツデータの配信を受ける構成であった。

【0 2 4 7】

しかしながら、図 2 1 に示したコンテンツデータ販売機 2 0 0 0 の構成において、コネクタ 2 0 1 0 の代わりに、メモリカード 1 1 0 との間のインターフェースのためのメモリスロットを設ける構成とすれば、携帯電話機 1 0 0 を介することなく、メモリカード 1 1 0 とコンテンツデータ販売機 2 0 0 0 とが直接データの授受を行なうことが可能である。

【0 2 4 8】

図 2 4 は、このような実施の形態 3 の変形例のコンテンツデータ販売機 2 0 0 1 の構成を示す概念図である。図 2 0 に示した実施の形態 3 のコンテンツデータ販売機 2 0 0 0 の構成と異なる点は、外部コネクタ 2 0 1 0 の代わりに、メモリカードを挿入できるカードスロット 2 0 3 0 が設けられ、このカードスロット 2 0 3 0 がインターフェース部 2 0 1 2 を介して、データバス B S 1 とデータの授受をする構成となっている点である。

【 0 2 4 9 】

図 2 5 および図 2 6 は、実施の形態 3 の変形例のデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

【 0 2 5 0 】

図 2 2 および図 2 3 に示した実施の形態 3 の配信モードとは、携帯電話機 1 0 0 を介さずに、メモ리카ード 1 1 0 とコンテンツデータ販売機 2 0 0 1 がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

【 0 2 5 1 】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

【 0 2 5 2 】

しかも、メモ리카ードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、コンテンツデータの再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

【 0 2 5 3 】

[実施の形態 4]

図 2 7 は、実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成を説明するための概略ブロック図である。図 2 1 に示したコンテンツデータ販売機 2 0 0 0 の構成と異なる点は、対象となるメモ리카ードが実施の形態 2 のメモ리카ード 1 2 0 であり、かつ使用される端末が携帯電話機 1 0 1 である点、およびこれに対応して、データ処理部 2 1 0 0 における暗号化処理部 3 2 2 は、K s 発生部 3 1 4 からのセッションキー K s に基づいてではなく、携帯電話機に装着されたメモ리카ードからセッションキー K s により暗号化されて送信され、復号処理部 3 1 8 により復号抽出されたセッションキー、たとえば、セッションキー K s 1 に基づいて、暗号化処理部 3 2 0 の出力をさらに暗号化して、データバス B S 1 を介してインターフェース部 2 0 1 2 およびコネクタ 2 0 1 0 に与える点である。

【 0 2 5 4 】

コンテンツデータ販売機 3 0 0 0 のその他の点は、図 2 1 に示した実施の形態

3 のコンテンツデータ販売機 2 0 0 0 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 2 5 5】

また、携帯電話機 1 0 1 およびメモリカード 1 1 0 の構成も実施の形態 2 で説明したものと同様であるので、その説明も繰り返さない。

【0 2 5 6】

図 2 8 および図 2 9 は、図 2 7 で説明したデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

【0 2 5 7】

図 2 8 および図 2 9 においては、ユーザ 1 が、メモリカード 1 2 0 を用いることで、コンテンツデータ販売機 3 0 0 0 から音楽データの配信を受ける場合の動作を説明している。

【0 2 5 8】

まず、ユーザが、コンテンツデータ販売機 3 0 0 0 のキーボード 2 0 0 4 のキーボタンの操作等によって、配信リクエストを指示する（ステップ S 5 0 0）。コンテンツデータ販売機 3 0 0 0 は、メモリカード 1 1 0 に対して公開暗号化鍵 K P m e d i a (1) の送信依頼を出力する（ステップ S 5 0 2）。

【0 2 5 9】

メモリカード 1 2 0 においては、この公開暗号化鍵 K P m e d i a (1) の送信依頼に応じて、K P m e d i a (1) 保持部 1 4 0 1 から、公開暗号化鍵 K P m e d i a (1) をコンテンツデータ販売機 3 0 0 0 に対して送信する（ステップ S 5 0 6）。さらに、メモリカード 1 2 0 においては、K s 1 発生部 1 4 3 2 によりセッションキー K s 1 が生成される（ステップ S 5 1 5）。

【0 2 6 0】

携帯電話機 1 0 1 がコンテンツデータ販売機 3 0 0 0 に公開暗号化鍵 K P m e d i a (1) を送信し（ステップ S 5 0 8）、コンテンツデータ販売機 3 0 0 0 が、メモリカード 1 2 0 から転送された公開暗号化鍵 K P m e d i a (1) を受信すると（ステップ S 5 1 0）、ディスプレイ 2 0 0 2 を介してユーザに料金投入を案内し、料金徴収を行なう（ステップ S 5 1 2）。続いて、コンテンツデー

タ販売機 3 0 0 0 は、セッションキー発生部 3 1 4 が、セッションキー K s を生成する。さらに、コンテンツデータ販売機 3 0 0 0 内の暗号化処理部 3 1 6 が、受信した公開暗号化鍵 K P m e d i a (1) により、このセッションキー K s を暗号化して暗号化セッションキー [K s] K m e d i a (1) を生成する（ステップ S 5 1 4 ）。

【 0 2 6 1 】

続いて、コンテンツデータ販売機 3 0 0 0 は、暗号化セッションキー [K s] K m e d i a (1) をデータバス B S 1 に与え、コネクタ 2 0 1 0 から出力する（ステップ S 4 1 6 ）。携帯電話機 1 0 1 は、この暗号化セッションキー [K s] K m e d i a (1) を受信すると、メモリカード 1 2 0 に転送する（ステップ S 5 1 8 ）。

【 0 2 6 2 】

メモリカード 1 2 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス B S 3 に与えられた暗号化セッションキー [K s] K m e d i a (1) を、復号処理部 1 4 0 4 が、秘密復号鍵 K m e d i a (1) により復号処理することにより、セッションキー K s を復号し抽出する（ステップ S 5 2 0 ）。

【 0 2 6 3 】

続いて、暗号化処理部 1 4 0 6 は、K P c a r d (1) 保持部 1 4 0 5 から与えられる公開暗号化鍵 K P c a r d (1) および K s 1 発生部 1 4 3 2 からのセッションキー K s 1 を、セッションキー K s により暗号化し（ステップ S 5 2 2 ）、データ [K P c a r d (1) 、 K s 1] K s を生成する（ステップ S 5 2 4 ）。

【 0 2 6 4 】

携帯電話機 1 0 1 は、暗号化処理部 1 4 0 6 により暗号化されたデータ [K P c a r d (1) 、 K s 1] K s をコンテンツデータ販売機 3 0 0 0 に対して送信する（ステップ S 5 2 6 ）。

【 0 2 6 5 】

コンテンツデータ販売機 3 0 0 0 では、コネクタ 2 0 1 0 を介してデータ [K P c a r d (1) 、 K s 1] K s が受信され（ステップ S 5 2 8 ）、データバス

B S 1 に与えられたデータ [K P c a r d (1) 、 K s 1] K s を復号処理部 3 1 8 が、セッションキー K s により復号処理して、公開暗号化鍵 K P c a r d (1) およびセッションキー K s 1 を復号抽出する (ステップ S 5 3 0) 。

【 0 2 6 6 】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する (ステップ S 5 3 2) 。

【 0 2 6 7 】

さらに、コンテンツデータ販売機 3 0 0 0 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、コネクタ 2 0 1 0 を介して、携帯電話機 1 0 1 に送信する (ステップ S 5 3 4) 。

【 0 2 6 8 】

携帯電話機 1 0 1 が暗号化コンテンツデータ [D c] K c を受信すると (ステップ S 5 3 6) 、メモリカード 1 2 0 においては、受信した暗号化コンテンツデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する (ステップ S 5 3 8) 。

【 0 2 6 9 】

一方、コンテンツデータ販売機 3 0 0 0 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し (ステップ S 5 4 0) 、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのライセンスキー K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられた公開暗号化鍵 K P c a r d (1) により暗号化処理する (ステップ S 5 4 2) 。

【 0 2 7 0 】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c 、 L i c e n s e] K c a r d (1) を受取って、さらにセッションキー K s 1 により暗号化したデータをデータバス B S 1 に与え、暗号化処理部 3 2 2 により暗号化されたデータ [[K c , L i c e n s e] K c a r d (1)] K s 1 が携帯電話機 1 0 1 に対して出力される (ステップ S 5 4 6) 。

【 0 2 7 1 】

携帯電話機 1 0 1 がデータ [[K c , L i c e n s e] K c a r d (1)] K

s 1 を受信すると（ステップ S 5 4 8）、メモリカード 1 2 0 においては、復号処理部 1 4 1 0 がセッションキー K s 1 により復号処理を行ない、データ [K c , L i c e n s e] K c a r d (1) を抽出し、メモリ 1 4 1 2 に格納する（ステップ S 5 5 2）。

【0 2 7 2】

以下の処理は、図 2 2 および図 2 3 に示した実施の形態 3 の処理と同様であるので、その説明は繰り返さない。

【0 2 7 3】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータ配信を受けることができる。

【0 2 7 4】

しかも、データバス上で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

【0 2 7 5】

[実施の形態 4 の変形例]

実施の形態 4 のデータ配信システムにおいては、メモリカード 1 2 0 は、携帯電話機 1 0 1 を介して、コンテンツデータ販売機 3 0 0 0 から暗号化コンテンツデータの配信を受ける構成であった。

【0 2 7 6】

しかしながら、図 2 7 に示したコンテンツデータ販売機 3 0 0 0 の構成において、実施の形態 3 の変形例と同様に、コネクタ 2 0 1 0 の代わりに、メモリカード 1 2 0 との間のインターフェースのためにメモリスロットを設ける構成とすれば、携帯電話機 1 0 1 を介することなく、メモリカード 1 2 0 とコンテンツデータ販売機 3 0 0 0 とが直接データの授受を行なうことが可能である。

【0 2 7 7】

このような実施の形態 4 の変形例のコンテンツデータ販売機 3 0 0 1 の構成は、データ処理部 2 1 0 0 の構成を除いて、図 2 4 に示した実施の形態 3 の変形例の構成と同様である。

【0 2 7 8】

すなわち、実施の形態 4 の変形例のコンテンツデータ販売機 3 0 0 1 の構成は、図 2 7 に示した実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成と異なり、外部コネクタ 2 0 1 0 の代わりに、メモ리카ードを挿入できるカードスロット 2 0 3 0 が設けられ、このカードスロット 2 0 3 0 がインターフェース部 2 0 1 2 を介して、データバス B S 1 とデータの授受をする構成となっている。

【0 2 7 9】

図 3 0 および図 3 1 は、実施の形態 4 の変形例のデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

【0 2 8 0】

図 2 8 および図 2 9 に示した実施の形態 3 の配信モードとは、携帯電話機 1 0 1 を介さずに、メモ리카ード 1 2 0 とコンテンツデータ販売機 3 0 0 1 がデータの授受をする点を除いては、同様の処理であるので、同一処理には同一符号を付して、その説明は繰り返さない。

【0 2 8 1】

以上のような構成および動作により、一層簡易に、ユーザは暗号化された音楽データ等の配信を受けることができる。

【0 2 8 2】

しかも、メモ리카ードが独立して、暗号化コンテンツデータの配信を受け、格納できるので、音楽の再生を行なう手段の選択の幅が広がり、よりユーザの利便性が向上するという利点もある。

【0 2 8 3】**[実施の形態 5]**

実施の形態 5 の配信サーバ 1 2、携帯電話機 1 0 5 およびメモ리카ード 1 4 0 は、以下に説明するように、実施の形態 2 の配信サーバ 1 1、携帯電話機 1 0 1 およびメモ리카ード 1 2 0 の構成とは、以下の点で異なることを特徴とする。

【0 2 8 4】

すなわち、実施の形態 5 の携帯電話機 1 0 5 では、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこの携帯電話機 1 0 5 を登録する際に

、この携帯電話機 1 0 5 に割当てられた公開暗号鍵 K P p および証明データ C r t f とを公開復号鍵（公開認証鍵） K P m a s t e r により暗号化された形で記録保持する手段を有している。

【 0 2 8 5 】

同様に、実施の形態 5 のメモリカード 1 4 0 でも、たとえば、あらかじめ配信システムにおける認証機構等の管理部門にこのメモリカード 1 4 0 を登録する際に、このメモリカードに割当てられた公開暗号鍵 K P m e d i a および証明データ C r t f とを公開復号鍵（公開認証鍵） K P m a s t e r により暗号化された形で記録保持する手段を有している。

【 0 2 8 6 】

ここで、メモリカード 1 4 0 および実施の形態 5 の配信サーバ 1 2 には、この公開復号鍵（公開認証鍵） K P m a s t e r を記録保持する手段を有している。この公開復号鍵（公開認証鍵） K P m a s t e r は、システム中でデータ出力を行なう全ての機器がセッションキーのやりとりに対して、相互にデータの授受を行なえる機器であることの証明と、セッションキーを相手方に送付する際に用いる暗号化鍵の獲得に用いるシステム共通の復号鍵である。

【 0 2 8 7 】

以下、さらに、実施の形態 5 の携帯電話機 1 0 5 、メモリカード 1 4 0 および配信サーバ 1 2 の構成をより詳しく説明する。

【 0 2 8 8 】

図 3 2 は、実施の形態 5 における携帯電話機 1 0 5 の構成を説明するための概略ブロック図である。

【 0 2 8 9 】

図 1 2 に示した実施の形態 2 の携帯電話機 1 0 1 の構成と異なる点は、 K P p 保持部 1 5 2 4 の替わりに、公開復号鍵（公開認証鍵） K P m a s t e r により暗号化された、公開暗号鍵 K P p および証明データ C r t f を保持するための [K P p , C r t f] K P m a s t e r 保持部 1 5 2 5 を備える構成となっていることである。

【 0 2 9 0 】

携帯電話機 1 0 5 のその他の点は、図 1 2 に示した実施の形態 2 の携帯電話機 1 0 1 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 2 9 1】

図 3 3 は、実施の形態 5 のメモリカード 1 4 0 に対応した配信サーバ 1 2 の構成を示す概略ブロック図である。図 1 1 に示した実施の形態 2 の配信サーバ 1 1 の構成と異なる点は、データ処理部 3 1 0 は、公開復号鍵 $KPmaster$ を保持する $KPmaster$ 保持部 3 2 4 と、 $KPmaster$ 保持部 3 2 4 から出力される公開復号鍵 $KPmaster$ に基づいて、通信網から通信装置 3 5 0 を介してデータバス $BS1$ に与えられるデータを復号するための復号処理部 3 2 6 とをさらに備える構成となっている点である。暗号化処理部 3 1 6 は、復号処理部 3 2 6 での復号処理により抽出された公開暗号化鍵 $KPmedia$ により、 Ks 発生部 3 1 4 で発生されたセッションキー Ks を暗号化し、また、配信制御部 3 1 2 は、復号処理部 3 2 6 での復号処理により抽出された証明データ $Crtf$ により、配信を求めてきたメモリカードおよび携帯電話機が正規であるかの認証を行なう。

【0 2 9 2】

配信サーバ 1 2 のその他の点は、図 1 2 に示した実施の形態 2 の配信サーバ 1 1 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 2 9 3】

図 3 4 は、本発明の実施の形態 5 のメモリカード 1 4 0 の構成を説明するための概略ブロック図であり、実施の形態 2 の図 1 3 と対比される図である。

【0 2 9 4】

実施の形態 5 のメモリカード 1 4 0 の構成が、実施の形態 2 のメモリカード 1 2 0 の構成と異なる点は、まず、メモリカード 1 4 0 は、公開暗号鍵 $KPmedia$ および証明データ $Crtf$ とを公開復号鍵（公開認証鍵） $KPmaster$ により暗号化された形で記録保持する $[KPmedia, Crtf] KPmaster$ 保持部 1 4 4 2 を備える構成となっていることである。一方で、切換えス

イッチ 1 4 3 6 は省略され、[K P m e d i a , C r t f] K P m a s t e r 保持部 1 4 4 2 の出力は直接データベース B S 3 に与えられる。

【0 2 9 5】

さらに、メモ리카ード 1 4 0 は、公開復号鍵 K P m a s t e r を記録保持するための K P m a s t e r 保持部 1 4 5 0 と、K P m a s t e r 保持部 1 4 5 0 から出力される公開復号鍵 K P m a s t e r に基づいて、データベース B S 3 上のデータを復号するための復号処理部 1 4 5 2 とを備える。

【0 2 9 6】

復号処理部 1 4 5 2 での復号処理により抽出される公開暗号化鍵 K P m e d i a および証明データ C r t f のうち、公開暗号化鍵 K P m e d i a は、暗号化処理部 1 4 3 0 に与えられ、証明データ C r t f は、データベース B S 5 を介して、コントローラ 1 4 2 0 に与えられる。

【0 2 9 7】

メモ리카ード 1 4 0 のその他の構成は、図 1 3 に示したメモ리카ード 1 2 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 2 9 8】

[配信モード]

図 3 5 および図 3 6 は、図 3 4 で説明したメモ리카ード 1 4 0 を用いた配信モードを説明するための第 1 および第 2 のフローチャートである。

【0 2 9 9】

図 3 5 および図 3 6 においても、ユーザ 1 が、メモ리카ード 1 4 0 を装着した携帯電話機 1 0 5 にて配信サーバ 1 2 からコンテンツデータの配信を受ける場合の動作を説明している。

【0 3 0 0】

まず、ユーザ 1 の携帯電話機 1 0 5 から、ユーザによりタッチキー 1 1 0 8 のキーボタンの操作等によって、配信リクエストがなされる（ステップ S 1 0 0 ）。

【0 3 0 1】

また、メモ리카ード 1 4 0 において保持される公開暗号化鍵 $KPmedia$ は、他のメモ리카ードにおける公開暗号化鍵 $KPmedia$ と区別するために公開暗号化鍵 $KPmedia(1)$ としている。さらに、メモ리카ード 1 4 0、携帯電話機 1 0 5 における証明データをそれぞれ $Crtf(1)$ 、 $Crtf(p)$ とする。

【0302】

メモ리카ード 1 4 0 においては、この配信リクエストに応じて、 $[KPmedia, Crtf]$ $KPmaster$ 保持部 1 4 4 2 から、公開暗号化鍵 $KPmedia(1)$ および証明データ $Crtf(1)$ を暗号化したデータ $[KPmedia(1), Crtf(1)]$ $KPmaster$ を携帯電話機 1 0 5 に対して出力する（ステップ S 1 0 2'）。

【0303】

携帯電話機 1 0 5 では、メモ리카ード 1 4 0 からのデータ $[KPmedia(1), Crtf(1)]$ $KPmaster$ とともに、 $[KPP, Crtf]$ $KPmaster$ 保持部 1 5 2 5 からのデータ $[KPP, Crtf(p)]$ $KPmaster$ 、配信リクエストを配信サーバ 1 2 に対して送信する（ステップ S 1 0 3）。

【0304】

配信サーバ 1 2 では、メモ리카ード 1 4 0 から転送された配信リクエストならびにデータ $[KPP, Crtf(p)]$ $KPmaster$ 、 $[KPmedia(1), Crtf(1)]$ $KPmaster$ を受信すると（ステップ S 1 0 4'）、公開復号鍵 $KPmaster$ により復号処理部 3 2 6 が復号処理を行い、証明データ $Crtf(1)$ 、 $Crtf(p)$ 、公開暗号化鍵 KPP 、公開暗号化鍵 $KPmedia(1)$ の抽出を行なう（ステップ S 1 0 5）。

【0305】

復号された証明データ $Crtf(1)$ および $Crtf(p)$ に基づいて、配信制御部 3 1 2 は、配信サーバ 1 2 に対して照会を行ない、メモ리카ードと携帯電話機の証明データ $Crtf(1)$ および $Crtf(p)$ がともに正規の証明データの場合は次の処理に移行し（ステップ S 1 0 6'）、いずれかが正規の証明デ

ータでない場合には、処理を終了する（ステップ S 1 5 4）。

【0 3 0 6】

照会の結果、正規の証明データであることが確認されると、配信サーバ 1 2 では、セッションキー発生部 3 1 4 が、セッションキー K s を生成する。さらに、配信サーバ 1 2 内の暗号化処理部 3 1 6 が、受信した公開暗号化鍵 K P m e d i a (1) により、このセッションキー K s を暗号化して暗号化セッションキー [K s] K m e d i a (1) を生成する（ステップ S 1 0 8）。

【0 3 0 7】

続いて、配信サーバ 1 2 は、暗号化セッションキー [K s] K m e d i a (1) をデータバス B S 1 に与える。通信装置 3 5 0 は、暗号化処理部 3 1 6 からの暗号化セッションキー [K s] K m e d i a (1) を、通信網を通じて、携帯電話機 1 0 5 のメモ리카ード 1 4 0 に対して送信する（ステップ S 1 1 0）。

【0 3 0 8】

携帯電話機 1 0 5 が、暗号化セッションキー [K s] K m e d i a (1) を受信すると（ステップ S 1 1 2）、メモ리카ード 1 4 0 においては、メモリインタフェース 1 2 0 0 を介して、データバス B S 3 に与えられた受信データを、復号処理部 1 4 0 4 が、秘密復号鍵 K m e d i a (1) で復号処理することにより、セッションキー K s を復号し抽出する（ステップ S 1 1 4）。

【0 3 0 9】

さらに、メモ리카ード 1 4 0 においては、K s 1 発生部 1 4 3 2 によりセッションキー K s 1 が生成される（ステップ S 1 1 5）。

【0 3 1 0】

続いて、配信モードにおいては、切換スイッチ 1 4 0 9 は、接点 P a または P b が順次閉じる状態が選択されるので、暗号化処理部 1 4 0 6 は、接点 P a を介してセッションキー発生部 1 4 3 2 から与えられるセッションキー K s 1 と接点 P b を介して K P c a r d (1) 保持部 1 4 0 5 から与えられる公開暗号化鍵 K P c a r d (1) （メモ리카ード 1 4 0 に対する公開暗号化鍵）とを、セッションキー K s により暗号化し（ステップ S 1 1 6）、データ [K P c a r d (1) 、 K s 1] K s を生成する（ステップ S 1 1 8）。

【0311】

携帯電話機 1 0 5 は、暗号化処理部 1 4 0 6 により暗号化されたデータ [K P c a r d (1)、K s 1] K s を配信サーバ 1 2 に対して送信する（ステップ S 1 2 0）。

【0312】

配信サーバ 1 2 では、通信装置 3 5 0 によりデータ [K P c a r d (1)、K s 1] K s が受信され（ステップ S 1 2 2）、データベース B S 1 に与えられたデータ [K P c a r d (1)、K s 1] K s を復号処理部 3 1 8 が、セッションキー K s により復号処理して、公開暗号化鍵 K P c a r d (1) およびセッションキー K s 1 を復号抽出する（ステップ S 1 2 4）。

【0313】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する（ステップ S 1 2 6）。

【0314】

さらに、配信サーバ 1 2 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、通信装置 3 5 0 を介して、メモリカード 1 4 0 に送信する（ステップ S 1 2 8）。

【0315】

携帯電話機 1 0 5 が暗号化コンテンツデータ [D c] K c を受信すると（ステップ S 1 3 0）、メモリカード 1 4 0 においては、受信した暗号化コンテンツデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する（ステップ S 1 3 2）。

【0316】

一方、配信サーバ 1 2 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し（ステップ S 1 3 4）、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのライセンスキー K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられた公開暗号化鍵 K P c a r d (1) により暗号化処理する（ステップ S 1 3 6）。

【0317】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [Kc, License] Kcard (1) を受取って、さらに、メモリカード 1 4 0 からのセッションキー Ks 1 により暗号化したデータをデータバス BS 1 に与える。通信装置 3 5 0 は、暗号化処理部 3 2 2 により暗号化されたデータ [[Kc, License] Kcard (1)] Ks 1 をメモリカード 1 4 0 に対して送信する。

【0 3 1 8】

携帯電話機 1 0 5 がデータ [[Kc, License] Kcard (1)] Ks 1 を受信すると (ステップ S 1 4 2)、メモリカード 1 4 0 においては、復号処理部 1 4 1 0 が接点 Pf を介して Ks 1 発生部 1 4 3 2 から与えられるセッションキー Ks 1 により復号処理を行ない、データ [Kc, License] Kcard (1) を抽出し、メモリ 1 4 1 2 に格納する (ステップ S 1 4 6)。

【0 3 1 9】

さらに、メモリカード 1 4 0 においては、コントローラ 1 4 2 0 により制御されて、復号処理部 1 4 1 6 が、メモリ 1 4 1 2 に格納されたデータ [Kc, License] Kcard (1) を復号し、復号されたライセンス情報データ License を、レジスタ 1 5 0 0 に格納する (ステップ 1 4 8)。

【0 3 2 0】

以上のような動作により、メモリカード 1 4 0 自身が、暗号化コンテンツデータを送る側 (配信サーバ 1 2) に、公開暗号化鍵 KPmedia (1) およびセッションキー Ks 1 を送信した上で、配信を受けることができ、メモリカード 1 4 0 は、音楽を再生可能な状態となる。

【0 3 2 1】

さらに、メモリカード 1 4 0 から配信サーバ 1 2 へは、配信受理が通知され、配信サーバ 1 2 で配信受理を受信すると (ステップ S 1 5 0)、課金データベース 3 0 2 にユーザ 1 の課金データが格納され (ステップ S 1 5 2)、処理が終了する (ステップ S 1 5 4)。

【0 3 2 2】

以上のような配信モードでは、メモリカードおよび携帯電話機の認証がなされ

た上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

【0 3 2 3】

[再生モード]

図 3 7 および図 3 8 は、携帯電話機 1 0 5 内において、メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽信号を復号化し、音楽として外部に出力するための再生処理を説明する第 1 および第 2 のフローチャートである。

【0 3 2 4】

図 3 7 および図 3 8 を参照して、携帯電話機 1 0 5 のタッチキー 1 1 0 8 等からのユーザ 1 の指示により、再生リクエストが携帯電話機 1 0 5 に対して出力される（ステップ S 2 0 0）。

【0 3 2 5】

これに応じて携帯電話機 1 0 5 からは、メモリカード 1 4 0 に対して、データ [K P p, C r t f (p)] K P m a s t e r が送信される（ステップ S 2 4 1）。

【0 3 2 6】

メモリカード 1 4 0 においては、データ [K P p, C r t f (p)] K P m a s t e r を受信すると、復号処理部 1 4 5 2 により復号処理が行われ、公開暗号化鍵 K P p およびデータ C r t f の抽出が行われる（ステップ S 2 4 3）。

【0 3 2 7】

抽出された証明データ C r t f に基づいて、コントローラ 1 4 2 0 は、携帯電話機 1 0 5 が正規の機器であるかを判断し（ステップ S 2 4 5）、正規の機器と判断した場合は、処理は次のステップ S 2 4 6 に移行し、正規の機器でないと判断した場合は、処理を終了する（ステップ S 2 8 0）。

【0 3 2 8】

正規の機器であると判断された場合、メモリカード 1 4 0 では、セッションキー K s 1 を生成する（ステップ S 2 4 6）。メモリカード 1 4 0 は、さらに、抽出された公開暗号化鍵 K P p によりセッションキー K s 1 を暗号化し（ステップ S 2 4 8）、生成された暗号化セッションキー [K s 1] K p を携帯電話機 1 0

5 に対して送信する（ステップ S 2 5 0）。

【0 3 2 9】

携帯電話機 1 0 5 では、メモリカード 1 4 0 からの暗号化セッションキー [K s 1] K p を受信すると、復号処理部 1 5 2 2 が、秘密復号鍵 K p により復号化してメモリカード 1 4 0 で生成したセッションキー K s 1 を抽出する（ステップ S 2 5 2）。続いて、K s 発生部 1 5 0 2 がセッションキー K s を生成し（ステップ S 2 5 3）、携帯電話機 1 0 5 の暗号化処理部 1 5 0 4 は、携帯電話機 1 0 5 で生成したセッションキー K s をセッションキー K s 1 により暗号化して、暗号化セッションキー [K s] K s 1 を生成し（ステップ S 2 5 4）、この暗号化セッションキー [K s] K s 1 をメモリカード 1 4 0 に対して送信する（ステップ S 2 5 6）。

【0 3 3 0】

メモリカード 1 4 0 は、データバス B S 2 を介して、携帯電話機 1 0 5 により生成され、かつ暗号化されたセッションキー K s を受け取り、セッションキー K s 1 により復号し、携帯電話機 1 0 5 で生成したセッションキー K s を抽出する（ステップ S 2 5 8）。

【0 3 3 1】

続いて、メモリカード 1 4 0 において、コントローラ 1 4 2 0 は、レジスタ 1 5 0 0 に保持されるライセンス情報データ L i c e n s e に基づいて、復号可能であるかを判断し（ステップ S 2 5 9）、復号可能と判断した場合は、次の処理に移行し、復号不可能と判断した場合は、処理を終了する（ステップ S 2 8 0）。

【0 3 3 2】

続いて、メモリカード 1 4 0 は、メモリ 1 4 1 2 から、暗号化されているデータ [K c, L i c e n s e] K c a r d (1) を読み出し、復号処理部 1 4 1 6 が復号処理を行なう（ステップ S 2 6 0）。

【0 3 3 3】

秘密復号鍵 K c a r d (1) により、メモリ 1 4 1 2 から読み出されたデータを復号可能な場合（ステップ S 2 6 2）、ライセンスキー K c が抽出される（ス

テップ S 2 6 4)。一方、復号不可能の場合、処理は終了する（ステップ S 2 8 0）。

【0 3 3 4】

メモリ 1 4 1 2 から読み出されたデータを復号可能な場合は、さらに、レジスタ 1 5 0 0 内のライセンス情報データ L i c e n s e のうち、再生回数に関するデータが変更される（ステップ S 2 6 6）。

【0 3 3 5】

続いて、メモリカード 1 4 0 においては、暗号化処理部 1 4 0 6 が、抽出したセッションキー K s により、ライセンスキー K c を暗号化し（ステップ S 2 6 8）、暗号化されたライセンスキー [K c] K s をデータバス B S 2 に与える（ステップ S 2 7 0）。

【0 3 3 6】

携帯電話機 1 0 5 の復号処理部 1 5 0 6 は、セッションキー K s により復号化処理を行なうことにより、ライセンスキー K c を取得する（ステップ S 2 7 2）。

【0 3 3 7】

続いて、メモリカード 1 4 0 は、暗号化コンテンツデータ [D c] K c をメモリ 1 4 1 2 から読み出し、データバス B S 2 に与える（ステップ S 2 7 4）。

【0 3 3 8】

携帯電話機 1 0 5 の音楽再生部 1 5 0 8 は、暗号化コンテンツデータ [D c] K c を、抽出されたライセンスキー K c により復号処理して平文のコンテンツデータを生成し（ステップ S 2 7 6）、コンテンツデータから音楽信号を再生して混合部 1 5 1 0 に与える（ステップ S 2 7 6）。デジタルアナログ変換部 1 5 1 2 は、混合部 1 5 1 0 からのデータを受け取って変換し、外部に再生された音楽を出力し、処理が終了する（ステップ S 2 3 2）。

【0 3 3 9】

このような構成とすることで、メモリカード自身および携帯電話自身が、それぞれセッションキー K s 1 または K s を生成し、これにより暗号化コンテンツデータの授受を行なった上で、再生動作を行なうことが可能となる。

【0 3 4 0】

さらに、メモリカード 1 4 0 が携帯電話機 1 0 5 の認証を行なった上で、再生動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

【0 3 4 1】

[移動または複製モード]

図 3 9 および図 4 0 は、2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 および第 2 のフローチャートである。

【0 3 4 2】

まず、携帯電話機 1 0 5 と同様の構成を有する携帯電話機 1 0 6 が送信側であり、携帯電話機 1 0 5 が受信側であるものとする。また、携帯電話機 1 0 6 にも、メモリカード 1 4 0 と同様の構成を有するメモリカード 1 4 2 が装着されているものとする。

【0 3 4 3】

携帯電話機 1 0 6 は、まず、携帯電話機 1 0 5 に対して、移動リクエストまたは複製リクエストを出力する（ステップ S 3 0 0）。

【0 3 4 4】

携帯電話機 1 0 5 がこのリクエストを受信すると（ステップ S 3 0 1）、メモリカード 1 4 2 は、これに応じて、メモリ 1 4 1 2 内の暗号化コンテンツデータ [D c] K c を読み出して、メモリカード 1 4 0 に対して出力し（ステップ S 3 0 2）、メモリカード 1 4 0 では、暗号化コンテンツデータ [D c] K c をメモリ 1 4 1 2 に格納する（ステップ S 3 0 4）。

【0 3 4 5】

続いて、携帯電話機 1 0 6 および 1 0 5 においては、ステップ S 3 0 0 において与えられたリクエストが、「移動リクエスト」であるか「複製リクエスト」であるかが判断され（ステップ S 3 0 6、ステップ S 3 0 6'）、「移動リクエスト」である場合、メモリカード 1 4 0 は、この移動リクエストに応じて、[K P m e d i a, C r t f] K P m a s t e r 保持部 1 4 4 2 から、公開暗号化鍵 K P m e d i a (1) および証明データ C r t f (1) を暗号化したデータ [K P

media (1), Crtf (1)] KPmaster を携帯電話機 105 に対して出力する (ステップ S307)。

【0346】

携帯電話機 105 では、メモリカード 140 からのデータ [KPmedia (1), Crtf (1)] KPmaster を携帯電話機 106 に対して送信する (ステップ S308)。

【0347】

携帯電話機 106 では、メモリカード 140 から転送されたデータ [KPmedia (1), Crtf (1)] KPmaster を受信すると (ステップ S309)、メモリカード 142 内の復号処理部 1452 が復号処理を行い、証明データ Crtf (1)、公開暗号化鍵 KPmedia (1) の抽出を行なう (ステップ S310)。

【0348】

復号された証明データ Crtf (1) に基づいて、コントローラ 1420 は、認証を行ない、正規メモリカードからのアクセスの場合は次の処理に移行し (ステップ S311)、正規メモリカードでない場合には、携帯電話機 106 は移動不可の通知を送信するとともに、メモリカード 142 は処理を終了する (ステップ S374)。携帯電話機 105 が移動不可通知を受信すると (ステップ S313)、メモリカード 140 も処理を終了する (ステップ S374)。

【0349】

一方、ステップ S311 での照会の結果、正規メモリカードであることが確認されると、メモリカード 142 の Ks2 発生回路 1432 は、セッションキー Ks2 を生成し (ステップ S314)、公開暗号化鍵 KPmedia (1) を用いて、暗号化処理部 1430 がセッションキー Ks2 を暗号化する (ステップ S315)。

【0350】

携帯電話機 106 は、暗号化セッションキー [Ks2] KPmedia (1) を携帯電話機 105 に対して送信する (ステップ S316)。携帯電話機 105 は、暗号化セッションキー [Ks2] KPmedia (1) を受信すると (ステ

ップ S 3 1 8)、メモリカード 1 4 0 に伝達し、メモリカード 1 4 0 は、復号処理部 1 4 0 4 が復号して、セッションキー K s 2 を受理する (ステップ S 3 2 0)。さらに、メモリカード 1 4 0 においてセッションキー K s 1 が生成される (ステップ S 3 2 1)。

【0 3 5 1】

メモリカード 1 4 0 においては、セッションキー K s 2 によりメモリカード 1 4 0 の公開暗号化鍵 K P c a r d (1) およびセッションキー K s 1 を暗号化して (ステップ S 3 2 2)、携帯電話機 1 0 5 から携帯電話機 1 0 6 に対して暗号化されたデータ [K P c a r d (1)、K s 1] K s 2 を送信する (ステップ S 3 2 4)。携帯電話機 1 0 6 は、データ [K P c a r d (1)、K s 1] K s 2 を受信し (ステップ S 3 2 6)、メモリカード 1 4 2 に転送する。

【0 3 5 2】

メモリカード 1 4 2 においては、復号処理部 1 4 1 0 が、メモリカード 1 4 0 から送信された暗号化データ [K P c a r d (1)、K s 1] K s 2 をセッションキー K s 2 により復号化して、メモリカード 1 4 0 の公開暗号化鍵 K P c a r d (1)、セッションキー K s 1 を復号抽出する (ステップ S 3 3 0)。

【0 3 5 3】

続いて、メモリカード 1 4 2 においては、メモリ 1 4 1 2 からメモリカード 1 4 2 の公開暗号化鍵 K P c a r d (2) により暗号化されているライセンスキー K c、ライセンス情報データ L i c e n s e に対応する [K c、L i c e n s e] K c a r d (2) 読出される (ステップ S 3 3 2)。

【0 3 5 4】

続いて、メモリカード 1 4 2 の復号処理部 1 4 1 6 が、秘密復号鍵 K c a r d (2) により、ライセンスキー K c、ライセンス情報データ L i c e n s e を復号処理する (ステップ S 3 3 4)。

【0 3 5 5】

メモリカード 1 4 2 のコントローラ 1 4 2 0 は、このようにして復号されたライセンス情報データ L i c e n s e の値を、レジスタ 1 5 0 0 内のデータ値と置換する (ステップ S 3 3 6)。

【0356】

さらに、メモリカード142の暗号化処理部1414は、復号処理部1410において抽出されたメモリカード140における公開暗号化鍵K P c a r d (1)により、ライセンスキーK c、ライセンス情報データL i c e n s eとを暗号化する(ステップS338)。

【0357】

メモリカード142の暗号化処理部1414により暗号化されたデータは、切換スイッチ1409(接点P dが閉じている)を介して、さらに、暗号化処理部1406に与えられ、メモリカード142の暗号化処理部1406は、データ[K c, L i c e n s e] K c a r d (1)をセッションキーK s 1により暗号化してデータ[[K c, L i c e n s e] K c a r d (1)] K s 1を生成する(ステップS340)。

【0358】

続いて、メモリカード142は、携帯電話機106に対してデータ[[K c, L i c e n s e] K c a r d (1)] K s 1を出力し(ステップS342)、携帯電話機106はデータ[[K c, L i c e n s e] K c a r d (1)] K s 1を携帯電話機105に対して送信する(ステップS344)。

【0359】

携帯電話機105が受信したデータ[[K c, L i c e n s e] K c a r d (1)] K s 1は(ステップS346)、メモリカード140に対して伝達され、メモリカード140の復号処理部1410は、暗号化されたデータ[[K c, L i c e n s e] K c a r d (1)] K s 1を復号して、データ[K c, L i c e n s e] K c a r d (1)を受理する(ステップS348)。

【0360】

メモリカード140においては、復号処理部1410により、セッションキーK s 1に基づいて復号化処理されたデータ[K c, L i c e n s e] K c a r d (1)をメモリ1412に格納する(ステップS350)。さらに、メモリカード140においては、復号処理部1416が、秘密復号鍵K c a r d (1)に基づいて、データ[K c, L i c e n s e] K c a r d (1)を復号し、復号され

たライセンス情報データ `L i c e n s e` をレジスタ 1 5 0 0 に格納する（ステップ S 3 5 2）。

【0 3 6 1】

以後の移動モードにおける処理ならびに複製モードにおけるメモ리카ード 1 4 0 および 1 4 2 の処理は、図 1 8 および図 1 9 で説明した実施の形態 2 のメモ리카ード 1 2 0、1 2 2 等の処理と同様であるので、その説明は繰り返さない。

【0 3 6 2】

このような構成とすることで、移動元および移動先のメモ리카ード自身が、セッションキーをそれぞれ生成した上で、移動動作を行なうこと、および複製動作を行なうことが可能となる。

【0 3 6 3】

したがって、データバス上で伝達されるデータの暗号化キーが、セッションごとに、かつ、機器ごとに変更されるので、データ授受のセキュリティが一層向上するという効果がある。

【0 3 6 4】

しかも、以上のような構成を用いることで、たとえば、メモ리카ード 1 4 2 からメモ리카ード 1 4 0 へのデータの移動を、上述したようなセッションキー発生回路 1 5 0 2 を有する携帯電話端末を介さずに、メモ리카ードとメモ리카ードとを接続可能なインターフェース機器により行なうことも可能となり、ユーザの利便性が一層向上するという効果がある。

【0 3 6 5】

ここで、移動モード時には、再生情報内の再生回数を制限するライセンス情報データについては、メモリ 1 4 1 2 に記録されたライセンス情報データを、レジスタ 1 5 0 0 にて再生の都度修正された再生回数を記録したライセンス情報データに変更することでライセンス情報データを更新する。このようにして、メモ리카ード間をコンテンツデータが移動しても、再生回数に制限があるコンテンツデータの再生回数は、配信時に決められた再生回数の制限を越えることがないようにすることが可能である。

【0 3 6 6】

しかも、メモリカード 1 4 2 がメモリカード 1 4 0 の認証を行った上で、移動動作を行なうため、システムのセキュリティおよび著作権の保護が向上する。

【0 3 6 7】

[実施の形態 6]

図 4 1 は、本発明の実施の形態 6 のコンテンツデータ販売機 3 0 1 0 の構成を示す概略ブロック図であり、実施の形態 4 の図 2 7 と対比される図である。

【0 3 6 8】

ただし、以下の説明では、実施の形態 5 で説明したメモリカード 1 4 0 との間のインターフェースのためにメモリスロット 2 0 3 0 を設ける構成とし、実施の形態 4 の変形例と同様に、携帯電話機 1 0 5 を介することなく、メモリカード 1 4 0 とコンテンツデータ販売機 3 0 1 0 とが直接データの授受を行なう構成であるものとする。

【0 3 6 9】

もちろん、コネクタ 2 0 1 0 により、携帯電話機 1 0 5 を介して、メモリカード 1 4 0 とコンテンツデータ販売機 3 0 1 0 とがデータの授受を行なう構成とすることも可能である。

【0 3 7 0】

したがって、コンテンツデータ販売機 3 0 1 0 の構成が、実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成と異なる点は、コネクタ 2 0 1 0 の代わりに、メモリスロット 2 0 3 0 が設けられていることと、データ処理部 2 1 0 0 は、公開復号鍵 K P m a s t e r を保持する K P m a s t e r 保持部 3 2 4 と、K P m a s t e r 保持部 3 2 4 から出力される公開復号鍵 K P m a s t e r に基づいて、通信網から通信装置 3 5 0 を介してデータバス B S 1 に与えられるデータを復号するための復号処理部 3 2 6 とをさらに備える構成となっている点である。暗号化処理部 3 1 6 は、復号処理部 3 2 6 での復号処理により抽出された公開暗号化鍵 K P m e d i a により、K s 発生部 3 1 4 で発生されたセッションキー K s を暗号化し、また、配信制御部 3 1 2 は、復号処理部 3 2 6 での復号処理により抽出された証明データ C r t f により、配信を求めてきたメモリカードが正規のメモリカードであるかの認証を行なう。

【0 3 7 1】

コンテンツデータ販売機 3 0 1 0 のその他の点は、図 2 7 に示した実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 3 7 2】

[配信モード]

図 4 2 および図 4 3 は、図 4 1 で説明したコンテンツデータ販売機 3 0 1 0 を用いたデータ配信システムにおける配信動作を説明するための第 1 および第 2 のフローチャートである。

【0 3 7 3】

図 4 2 および図 4 3 においては、ユーザ 1 が、メモリカード 1 4 0 を用いることで、コンテンツデータ販売機 3 0 1 0 からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

【0 3 7 4】

まず、ユーザが、コンテンツデータ販売機 3 0 1 0 のキーボード 2 0 0 4 のキーボタンの操作等によって、配信リクエストを指示する（ステップ S 5 0 0）。

【0 3 7 5】

コンテンツデータ販売機 3 0 1 0 からは、メモリカード 1 4 0 に対して、認証のためのデータ [K P m e d i a , C r t f] K P m a s t e r の送信依頼が出力される（ステップ S 5 0 2'）。

【0 3 7 6】

メモリカード 1 4 0 においては、この送信依頼に応じて、[K P m e d i a , C r t f] K P m a s t e r 保持部 1 4 4 2 から、公開暗号化鍵 K P m e d i a (1) および証明データ C r t f (1) を暗号化したデータ [K P m e d i a (1) , C r t f (1)] K P m a s t e r をコンテンツデータ販売機 3 0 1 0 に対して出力する（ステップ S 5 0 7）。

【0 3 7 7】

コンテンツデータ販売機 3 0 1 0 では、メモリカード 1 4 0 から転送されたデータ [K P m e d i a (1) , C r t f (1)] K P m a s t e r を受信すると

、公開復号鍵K P m a s t e rにより復号処理部326が復号処理を行い、証明データC r t f (1)、公開暗号化鍵K P p、公開暗号化鍵K P m e d i a (1)の抽出を行なう(ステップS509)。

【0378】

復号された証明データC r t f (1)に基づいて、配信制御部312は、正規メモリカードからのアクセスかどうかの判断を行なう。正規のメモリカードの場合は次の処理に移行し(ステップS511)、正規メモリカードでない場合には、管理サーバ2200中の管理データベースに異常終了記録を格納し(ステップS561)、処理を終了する(ステップS562)。

【0379】

コンテンツデータ販売機3010は、ステップS511での照会の結果、正規メモリカードであることが確認されると、ディスプレイ2002を介してユーザーに料金投入を案内し、料金徴収を行なう(ステップS512)。

【0380】

続いて、コンテンツデータ販売機3010は、セッションキー発生部314が、セッションキーK sを生成する。さらに、コンテンツデータ販売機3010内の暗号化処理部316が、受信した公開暗号化鍵K P m e d i a (1)により、このセッションキーK sを暗号化して暗号化セッションキー[K s] K m e d i a (1)を生成する(ステップS514)。

【0381】

続いて、コンテンツデータ販売機3010は、暗号化セッションキー[K s] K m e d i a (1)をデータベースB S 1に与え、カードスロット2030から出力する(ステップS516)。

【0382】

メモリカード140においては、メモリインタフェース1200を介して、データベースB S 3に与えられた暗号化セッションキー[K s] K m e d i a (1)を、復号処理部1404が、秘密復号鍵K m e d i a (1)により復号処理することにより、セッションキーK sを復号し抽出する(ステップS520)。さらに、メモリカード140では、セッションキーK s 1が生成される(ステップS

5 2 1)。

【0 3 8 3】

続いて、配信モードにおいては、切換スイッチ 1 4 0 8 は、接点 P a が閉じる状態が選択されているので、暗号化処理部 1 4 0 6 は、接点 P a を介して K P c a r d (1) 保持部 1 4 0 5 から与えられる公開暗号化鍵 K P c a r d (1) を、セッションキー K s により暗号化し (ステップ S 5 2 2)、データ [K P c a r d (1)] K s を生成する (ステップ S 5 2 4)。

【0 3 8 4】

コンテンツデータ販売機 3 0 1 0 では、カードスロット 2 0 3 0 を介してデータ [K P c a r d (1)] K s が受信され (ステップ S 5 2 8)、データバス B S 1 に与えられたデータ [K P c a r d (1)] K s を復号処理部 3 1 8 が、セッションキー K s により復号処理して、公開暗号化鍵 K P c a r d (1) を復号抽出する (ステップ S 5 3 0)。

【0 3 8 5】

続いて、配信制御部 3 1 2 は、配信情報データベース 3 0 4 等に保持されているデータを元に、ライセンス I D データ等を含むライセンス情報データ L i c e n s e を生成する (ステップ S 5 3 2)。

【0 3 8 6】

さらに、コンテンツデータ販売機 3 0 1 0 は、暗号化コンテンツデータ [D c] K c を配信情報データベース 3 0 4 より取得して、カードスロット 2 0 3 0 を介して、メモリカード 1 4 0 に送信する (ステップ S 5 3 4)。

【0 3 8 7】

メモリカード 1 4 0 においては、受信した暗号化コンテンツデータ [D c] K c をそのままメモリ 1 4 1 2 に格納する (ステップ S 5 3 8)。

【0 3 8 8】

一方、コンテンツデータ販売機 3 0 1 0 は、ライセンスキー K c を配信情報データベース 3 0 4 より取得し (ステップ S 5 4 0)、暗号化処理部 3 2 0 は、配信制御部 3 1 2 からのライセンスキー K c とライセンス情報データ L i c e n s e とを、復号処理部 3 1 8 より与えられた公開暗号化鍵 K P c a r d (1) によ

り暗号化処理する（ステップ S 5 4 2）。

【0 3 8 9】

暗号化処理部 3 2 2 は、暗号化処理部 3 2 0 により暗号化されたデータ [K c、L i c e n s e] K c a r d (1) を受取って、さらにセッションキー K s により暗号化したデータをデータバス B S 1 に与え、暗号化処理部 3 2 2 により暗号化されたデータ [[K c, L i c e n s e] K c a r d (1)] K s 1 がメモ리카ード 1 4 0 に対して送信される（ステップ S 5 4 6）。

【0 3 9 0】

メモ리카ード 1 4 0 においては、復号処理部 1 4 1 0 がセッションキー K s 1 により復号処理を行ない、データ [K c, L i c e n s e] K c a r d (1) を抽出し、メモリ 1 4 1 2 に格納する（ステップ S 5 5 2）。

【0 3 9 1】

さらに、メモ리카ード 1 4 0 においては、コントローラ 1 4 2 0 により制御されて、復号処理部 1 4 1 6 が、メモリ 1 4 1 2 に格納されたデータ [K c, L i c e n s e] K c a r d (1) を復号し、復号されたライセンス情報データ L i c e n s e を、レジスタ 1 5 0 0 に格納する（ステップ S 5 5 4）。

【0 3 9 2】

以上のような動作により、メモ리카ード 1 4 0 は、コンテンツデータから音楽を再生可能な状態となる。

【0 3 9 3】

さらに、メモ리카ード 1 4 0 からコンテンツデータ販売機 3 0 1 0 へは、配信受理が通知され（ステップ S 5 5 8）、コンテンツデータ販売機 3 0 1 0 で配信受理を受信すると、管理サーバ 2 2 0 0 中の管理データベースに販売記録が送信され（ステップ S 5 6 0）、処理が終了する（ステップ S 5 6 2）。

【0 3 9 4】

以上のような構成により、ユーザは、より簡易に暗号化された音楽データ等のコンテンツデータの配信を受けることができる。しかも、メモ리카ードの認証がなされた上でコンテンツデータの配信が行われるので、システムのセキュリティおよび著作権の保護がより強化される。

【0 3 9 5】**[実施の形態 7]**

図 4 4 は、実施の形態 7 における携帯電話機 1 0 7 の構成を説明するための概略ブロック図である。

【0 3 9 6】

図 3 2 に示した実施の形態 5 の携帯電話機 1 0 5 の構成と異なる点は、携帯電話機という再生装置に共通な復号鍵 K c o m を保持する K c o m 保持部 1 5 3 0 と、復号処理部 1 5 0 6 の出力を受けて、復号鍵 K c o m について復号し、音楽再生部 1 5 0 8 にライセンスキー K c を与える復号処理部 1 5 3 2 とを備える構成となっていることである。

【0 3 9 7】

携帯電話機 1 0 7 のその他の点は、図 3 2 に示した実施の形態 5 の携帯電話機 1 0 5 の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。メモリカード 1 4 0 の構成も同様である。

【0 3 9 8】

すなわち、実施の形態 7 では、実施の形態 5 において、音楽再生部 1 5 0 8 に最終的にライセンスキー K c と与えられる以前において、システムを構成する機器間で授受されていたライセンスキー K c を、実施の形態 7 では、さらに暗号化した [K c] K c o m という状態でやり取りする以外は、実施の形態 5 の構成と同様である。

【0 3 9 9】

なお、以下の説明では、復号鍵 K c o m は共通鍵であるものとして説明するが、本発明はこのような場合に限定されず、たとえば、暗号化は公開鍵 K P c o m で行い、復号化を公開暗号化鍵 K P c o m とは非対称な秘密復号鍵 K c o m で行なう構成としてもよい。

【0 4 0 0】

図 4 5 は、実施の形態 7 の携帯電話機 1 0 7 に対応した配信サーバ 1 3 の構成を示す概略ブロック図である。図 3 3 に示した実施の形態 5 の配信サーバ 1 2 の構成と異なる点は、データ処理部 3 1 0 は、復号鍵 K c o m を保持する K c o m

保持部 3 3 0 と、配信制御部 3 1 2 を介して配信情報データベース 3 0 4 から与えられるライセンスキー K c を復号鍵 K c o m により暗号化処理して、暗号化ライセンスキー [K c] K c o m として暗号化処理部 3 2 0 に与える暗号化処理部 3 3 2 をさらに備える構成となっている点である。

【0 4 0 1】

配信サーバ 1 3 のその他の点は、図 3 3 に示した実施の形態 5 の配信サーバ 1 2 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 4 0 2】

[配信モード]

図 4 6 および図 4 7 は、図 4 4 および 4 5 で説明した配信サーバ 1 3 と携帯電話機 1 0 7 を用いた配信モードを説明するための第 1 および第 2 のフローチャートである。

【0 4 0 3】

図 4 6 および図 4 7 においても、ユーザ 1 が、メモリカード 1 4 0 を用いることで、配信サーバ 1 3 からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

【0 4 0 4】

ただし、図 4 6 および図 4 7 の処理は、ステップ S 1 3 4 において、配信サーバ 1 3 が、ライセンスキー K c を配信情報データベース 3 0 4 より取得した後、暗号化処理部 3 3 2 がキー K c を暗号化して（ステップ S 1 3 5）、以後は、暗号化ライセンスキー [K c] K c o m として授受される点を除いては、図 3 5 および図 3 6 で説明した実施の形態 5 の配信モードと同様であるので、その説明は繰り返さない。

【0 4 0 5】

以上のような配信モードでは、実施の形態 5 に比べて、さらにシステムのセキュリティが強化される。

【0 4 0 6】

[再生動作]

図 4 8 および図 4 9 は、携帯電話機 1 0 7 内において、メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽信号を再生し、音楽として外部に出力するための再生処理を説明する第 1 および第 2 のフローチャートである。

【0 4 0 7】

ただし、図 4 8 および図 4 9 に示した再生処理は、ステップ S 2 6 4 でメモリカード 1 4 0 のメモリ 1 4 1 2 から読み出されるキーが、暗号化ライセンスキー [K c] K c o m であり、以後、暗号化ライセンスキー [K c] K c o m として携帯電話機 1 0 7 に送信され、携帯電話機 1 0 7 において、ステップ S 2 7 3 で復号処理部 1 5 3 2 によりキー [K c] K c o m が復号されライセンスキー K c が音楽再生部 1 5 0 8 に与えられる点以外は、図 3 7 および図 3 8 に示した実施の形態 5 の再生処理と同様であるのでその説明は繰り返さない。

【0 4 0 8】

このような構成とすることで、再生モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

【0 4 0 9】

[移動または複製モード]

図 5 0 および図 5 1 は、実施の形態 7 において、2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 および第 2 のフローチャートである。

【0 4 1 0】

ただし、図 5 0 および図 5 1 の処理は、ライセンスキー K c が、暗号化ライセンスキー [K c] K c o m として授受される点を除いては、図 3 9 および図 4 0 で説明した実施の形態 5 の移動または複製モードの動作と同様であるので、その説明は繰り返さない。

【0 4 1 1】

このような構成とすることで、移動または複製モードにおけるシステムのセキュリティおよび著作権の保護が一層向上する。

【0 4 1 2】

[実施の形態 8]

図 5 2 は、本発明の実施の形態 8 のコンテンツデータ販売機 3 0 2 0 の構成を示す概略ブロック図であり、実施の形態 6 の図 4 1 と対比される図である。

【0 4 1 3】

コンテンツデータ販売機 3 0 2 0 の構成が、実施の形態 6 のコンテンツデータ販売機 3 0 1 0 の構成と異なる点は、データ処理部 2 1 0 0 は、復号鍵 K c o m を保持する K c o m 保持部 3 3 0 と、配信制御部 3 1 2 を介して配信情報データベース 3 0 4 から与えられるライセンスキー K c を復号鍵 K c o m により暗号化処理して、暗号化ライセンスキー [K c] K c o m として暗号化処理部 3 2 0 に与える暗号化処理部 3 3 2 をさらに備える構成となっている点である。

【0 4 1 4】

コンテンツデータ販売機 3 0 2 0 のその他の点は、図 4 1 に示した実施の形態 6 のコンテンツデータ販売機 3 0 1 0 の構成の構成と同様であるので、同一部分には同一符号を付してその説明は繰り返さない。

【0 4 1 5】

もちろん、実施の形態 8 でも、コネクタ 2 0 1 0 により、携帯電話機 1 0 7 を介して、メモリカード 1 4 0 とコンテンツデータ販売機 3 0 2 0 とがデータの授受を行なう構成とすることも可能である。

【0 4 1 6】

[配信モード]

図 5 3 および図 5 4 は、図 5 2 で説明したコンテンツデータ販売機 3 0 2 0 を用いたデータ配信システムにおける配信モードを説明するための第 1 および第 2 のフローチャートである。

【0 4 1 7】

図 5 3 および図 5 4 においては、ユーザ 1 が、メモリカード 1 4 0 を用いることで、コンテンツデータ販売機 3 0 2 0 からコンテンツデータ（音楽データ）の配信を受ける場合の動作を説明している。

【0 4 1 8】

ただし、図 5 3 および図 5 4 の処理は、ステップ S 5 4 0 において、コンテンツデータ販売機 3 0 2 0 が、ライセンスキー K c を配信情報データベース 3 0 4

より取得した後、暗号化処理部 3 3 2 がライセンスキー K c を暗号化して（ステップ S 5 4 1）、以後は、暗号化ライセンスキー [K c] K c o m として授受される点を除いては、図 4 2 および図 4 3 で説明した実施の形態 5 の配信動作と同様であるので、その説明は繰り返さない。

【0 4 1 9】

以上のような配信モードでは、実施の形態 6 に比べて、さらにシステムのセキュリティが強化される。

【0 4 2 0】

ここでは暗号化コンテンツデータを配信し、メモリカード 1 1 0、1 2 0、1 4 0 内のメモリ 1 4 1 2 に格納した後、ライセンスキー K c、ライセンス情報データ L i c e n s e の配信を受けるように説明したが、逆にライセンスキー K c、ライセンス情報データ L i c e n s e を配信し、メモリカード 1 1 0、1 2 0、1 4 0 内のレジスタ 1 5 0 0 に格納した後、暗号化コンテンツデータの配信を受けても構わない。

【0 4 2 1】

さらに、移動モードにおいても配信モードと同様に、暗号化コンテンツデータ、ライセンスキー K c、ライセンス情報データ L i c e n s e のいずれの移動が先であっても構わない。

【0 4 2 2】

なお、以上説明してきた各実施の形態において、配信データとしてコンテンツデータに付随する非暗号化データ、たとえば、上記音楽データの曲名、実演者（歌手、演奏家等）、作曲家、作詞家等の当該音楽データ（コンテンツデータ）に関する著作情報や配信サーバ 1 0、1 1、コンテンツデータ販売機 3 0 0 0、3 0 0 1 に対してアクセスするための情報等を、付加データ D i として暗号化コンテンツデータと併せて配信することも可能である。この付加データ D i は、配信、移動、複製においてはコンテンツデータとともに処理され、再生時には分離されてコンテンツデータとは個別にアクセス可能となるように、暗号化コンテンツデータと同じメモリ 1 4 1 2 に格納される。

【0 4 2 3】

〔実施の形態 9〕

図 5 5 は、以上説明してきたメモリカード 1 1 0, 1 2 0, 1 4 0 等の端子 1 2 0 2 部分の構成を説明する概略ブロック図である。

【0 4 2 4】

以下では、メモリカード 1 4 0 の端子 1 2 0 2 部分の構成であるものとして説明する。

【0 4 2 5】

メモリカード 1 4 0 には、端子 1 2 0 2 からシリアルにデータやコマンドが与えられる。これに対して、メモリカード 1 4 0 中のデータバス B S 3 には、パラレルにデータやコマンドが伝達されるものとする。

【0 4 2 6】

図 5 5 は、このようなメモリカード 1 4 0 へのデータ入力時のシリアル・パラレル変換と、データ出力時のパラレル・シリアル変換を行なう構成を示す概略ブロック図である。

【0 4 2 7】

端子 1 2 0 2 中のデータピン 1 4 6 0 には、データ入出力のタイミングを指定するための信号である信号 C S が与えられる。たとえば、信号 C S が活性化（“L” レベル）となった後の所定期間後に、データ入力ピン 1 4 6 2 に与えられるデータが“L” レベルとなることで、データ入力のタイミングが検出される。どのように、信号 C S が活性化（“L” レベル）となった後の所定期間後に、データ出力ピン 1 4 6 4 に出力されるデータが“L” レベルとなることで、データ出力のタイミングが検出される。インターフェースコントローラ 1 4 9 0 は、メモリカード 1 4 0 の外部からデータバス B S 3 へのデータ入力、およびデータバス B S 3 からメモリカード 1 4 0 外部へのデータ出力を管理する。

【0 4 2 8】

データ入力時は、データ入力ピン 1 4 6 2 に与えられたデータは、バッファ 1 4 6 8 を介して、縦列に接続された D-フリップフロップ 1 4 7 0. 0 ~ 1 4 7 0. 7 に入力される。すなわち、8 ビット分のデータが入力された時点で、D-フリップフロップ 1 4 7 0. 0 ~ 1 4 7 0. 7 の全てのデータが更新され、その

時点で、インターフェースコントローラ 1 4 9 0 により制御されて、データバッファ 1 4 2 7 . 0 ~ 1 4 2 7 . 7 からデータバス B S 3 へデータが平行に出力される。

【0 4 2 9】

データ出力時は、データバス B S 3 からのデータがマルチプレクサ 1 4 7 6 . 1 ~ 1 4 7 6 . 7 を介して、平行に与えられ D - フリップフロップ 1 4 7 4 . 0 ~ 1 4 7 4 . 7 に格納される。その後インターフェースコントローラ 1 4 9 0 により制御されて、マルチプレクサ 1 4 7 6 . 1 ~ 1 4 7 6 . 7 の接続が切り換えられ、D - フリップフロップ 1 4 7 4 . 0 ~ 1 4 7 4 . 7 が縦列に接続される。この状態で、D - フリップフロップ 1 4 7 4 . 0 ~ 1 4 7 4 . 7 のそれぞれに格納されたデータが、順次シリアルに、インターフェースコントローラ 1 4 9 0 により制御される出力バッファ 1 4 7 0 を介して、データ出力ピン 1 4 6 4 から出力される。

【0 4 3 0】

[実施の形態 9 の変形例]

図 5 6 は、データ入力速度を向上させるために、データ入力ピンの本数を 1 本から 2 本または 4 本に可変とすることが可能な、メモリカード 1 4 0 の端子 1 2 0 2 部分の構成の変形例を説明するための概略ブロック図である。

【0 4 3 1】

図 5 5 に示した構成と異なる点は、まず、4 本のデータ入力ピン 1 4 6 2 . 0 ~ 1 4 6 2 . 3 およびそれらに対応する入力バッファ 1 4 6 8 . 0 ~ 1 4 6 8 . 3 が設けられていることと、これらデータ入力ピン 1 4 6 2 . 0 ~ 1 4 6 2 . 3 に与えられたコマンドを入力バッファ 1 4 6 8 . 0 ~ 1 4 6 8 . 3 からインターフェースコントローラ 1 4 9 0 に伝達するためのマルチプレクサ 1 4 6 7 と、データ入力ピン 1 4 6 2 . 0 ~ 1 4 6 2 . 3 に与えられたデータまたはコマンドを、入力バッファ 1 4 6 8 . 0 ~ 1 4 6 8 . 3 から D - フリップフロップ 1 4 7 0 . 0 ~ 1 4 7 0 . 7 に選択的に与えるためのマルチプレクサ 1 4 6 9 . 1 ~ 1 4 6 9 . 7 とをさらに備える構成となっていることである。

【0 4 3 2】

次に動作について簡単に説明する。

電源投入後には、たとえば、メモリカード 1 4 0 は、1 本のデータ入力ピン 1 4 6 2 . 0 からのみデータ入力を受けつける状態となっている。

【0 4 3 3】

以下では、外部からデータ入力ピン 1 4 6 2 . 0 ~ 1 4 6 2 . 3 およびマルチプレクサ 1 4 6 7 を経由してインターフェースコントローラ 1 4 9 0 に与えられたコマンドにより、インターフェースコントローラ 1 4 9 0 がマルチプレクサ 1 4 6 9 . 1 ~ 1 4 6 9 . 7 を制御することで、4 本のデータ入力ピン 1 4 6 2 . 0 ~ 1 4 6 2 . 3 からデータを平行に入力するモードに動作モードが変更されたものとする。

【0 4 3 4】

まず、第 1 のタイミングで 4 本のデータ入力ピン 1 4 6 2 . 0 ~ 1 4 6 2 . 3 に与えられたデータは、マルチプレクサ 1 4 6 9 . 1 ~ 1 4 6 9 . 3 を経由して D-フリップフロップ 1 4 7 0 . 0 ~ 1 4 7 0 . 3 に与えられる。

【0 4 3 5】

次の第 2 のタイミングで、マルチプレクサ 1 4 6 9 . 1 ~ 1 4 6 9 . 7 の接続が切換わり、D-フリップフロップ 1 4 7 0 . 0 ~ 1 4 7 0 . 3 の出力がそれぞれ、D-フリップフロップ 1 4 7 0 . 4 ~ 1 4 7 0 . 7 に与えられて格納される。さらに第 3 のタイミングで、4 本のデータ入力ピン 1 4 6 2 . 0 ~ 1 4 6 2 . 3 に与えられたデータは、マルチプレクサ 1 4 6 9 . 1 ~ 1 4 6 9 . 3 を経由して D-フリップフロップ 1 4 7 0 . 0 ~ 1 4 7 0 . 3 に与えられる。

【0 4 3 6】

以上で、8 ビット分のデータの D-フリップフロップ 1 4 7 0 . 0 ~ 1 4 7 0 . 7 への格納が終了する。以後は、図 5 5 の場合と同様に、データバス B S 3 に対して平行に 8 ビット分のデータが与えられる。

【0 4 3 7】

データ出力の際の動作は、図 5 5 の場合と同様である。

以上のような構成により、データ配信時、特にコンテンツデータ販売機 2 0 0 0 等からコンテンツデータを購入する際のメモリカード 1 4 0 へのデータ配信時

間を短縮することが可能である。

【0 4 3 8】

また、以上説明した各実施の形態のうち、2つの携帯電話にそれぞれ装着された2つのメモリカード間で、たとえば、PHSのトランシーバモード等を利用することにより、コンテンツデータの移動を行なう処理を説明した実施の形態においては、このような構成に限定されず、たとえば、1つの携帯電話機に複数のメモリカードが同時装着可能な場合は、当該携帯電話機に2つのメモリカードを同時に装着することで、コンテンツデータの移動を行なう構成とすることも可能である。このようなコンテンツデータの移動の場合は、以上説明した各実施の形態において、2つの携帯電話機間での送受信のやりとりを省略すればよい。

【0 4 3 9】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【0 4 4 0】

【発明の効果】

以上説明したとおり、本願発明にかかる配信システムでは、正規のユーザのみがコンテンツデータを受信してメモリ中に格納することが可能となり、かつ、1度メモリカード中に格納されたデータを、他人にコピーさせる場合は、当該他人が再生可能な状態でデータを移植するためには、送信元においては、データの再生が不能となってしまう構成となっているので、無制限なコピーにより著作権が不当な不利益を被るのを防止することが可能となる。

【0 4 4 1】

また、ユーザが配信キャリアを介してではなく、コンテンツデータ販売機により暗号化コンテンツデータを購入することができるので、ユーザの利便性が一層向上する。

【図面の簡単な説明】

【図 1】 本発明の情報配信システムの全体構成を概略的に説明するための

概念図である。

【図 2】 図 1 に示した情報配信システムにおいて使用される通信のためのキーデータ（鍵データ）等の特性をまとめて説明する図である。

【図 3】 図 1 に示した配信サーバ 1 0 の構成を示す概略ブロック図である。

【図 4】 図 1 に示した携帯電話機 1 0 0 の構成を説明するための概略ブロック図である。

【図 5】 図 4 に示したメモ리카ード 1 1 0 の構成を説明するための概略ブロック図である。

【図 6】 図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 7】 図 1 および図 3 ～図 5 で説明したデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 8】 携帯電話機 1 0 0 内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明するフローチャートである。

【図 9】 2 つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

【図 1 0】 2 つのメモ리카ード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

【図 1 1】 実施の形態 2 のメモ리카ード 1 2 0 に対応した音楽サーバ 3 1 の構成を示す概略ブロック図である。

【図 1 2】 実施の形態 2 における携帯電話機 1 0 1 の構成を説明するための概略ブロック図である。

【図 1 3】 本発明の実施の形態 2 のメモ리카ード 1 2 0 の構成を説明するための概略ブロック図である。

【図 1 4】 図 1 3 で説明したメモ리카ード 1 2 0 を用いた配信モードを説明するための第 1 のフローチャートである。

【図 1 5】 図 1 3 で説明したメモリカード 1 2 0 を用いた配信モードを説明するための第 2 のフローチャートである。

【図 1 6】 携帯電話機 1 0 1 内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第 1 のフローチャートである。

【図 1 7】 携帯電話機 1 0 1 内においてコンテンツデータを再生し、音楽として外部に出力するための再生処理を説明する第 2 のフローチャートである。

【図 1 8】 2 つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

【図 1 9】 2 つのメモリカード間でコンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

【図 2 0】 実施の形態 3 のデータ配信システムの構成を説明するための概念図である。

【図 2 1】 実施の形態 3 のコンテンツデータ販売機 2 0 0 0 の構成を示す概略ブロック図である。

【図 2 2】 図 2 0 および図 2 1 で説明したデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 2 3】 図 2 0 および図 2 1 で説明したデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 2 4】 実施の形態 3 の変形例のコンテンツデータ販売機 2 0 0 1 の構成を示す概念図である。

【図 2 5】 実施の形態 3 の変形例のデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 2 6】 実施の形態 3 の変形例のデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 2 7】 実施の形態 4 のコンテンツデータ販売機 3 0 0 0 の構成を説明するための概略ブロック図である。

【図 2 8】 図 2 7 で説明したデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 2 9】 図 2 7 で説明したデータ配信システムにおける配信モードを説

明するための第 2 のフローチャートである。

【図 3 0】 実施の形態 4 の変形例のデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 3 1】 実施の形態 4 の変形例のデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 3 2】 実施の形態 5 における携帯電話機 1 0 5 の構成を説明するための概略ブロック図である。

【図 3 3】 実施の形態 5 のメモリカード 1 4 0 に対応した配信サーバ 1 2 の構成を示す概略ブロック図である。

【図 3 4】 本発明の実施の形態 5 のメモリカード 1 4 0 の構成を説明するための概略ブロック図である。

【図 3 5】 メモリカード 1 4 0 を用いた配信モードを説明するための第 1 のフローチャートである。

【図 3 6】 メモリカード 1 4 0 を用いた配信モードを説明するための第 2 のフローチャートである。

【図 3 7】 メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第 1 のフローチャートである。

【図 3 8】 メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第 2 のフローチャートである。

【図 3 9】 2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

【図 4 0】 2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

【図 4 1】 本発明の実施の形態 6 のコンテンツデータ販売機 3 0 1 0 の構成を示す概略ブロック図である。

【図 4 2】 コンテンツデータ販売機 3 0 1 0 を用いたデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 4 3】 コンテンツデータ販売機 3 0 1 0 を用いたデータ配信システムにおける配信モードを説明するための第 2 のフローチャートである。

【図 4 4】 実施の形態 7 における携帯電話機 1 0 7 の構成を説明するための概略ブロック図である。

【図 4 5】 実施の形態 7 の携帯電話機 1 0 7 に対応した配信サーバ 1 3 の構成を示す概略ブロック図である。

【図 4 6】 配信サーバ 1 2 と携帯電話機 1 0 7 を用いた配信モードを説明するための第 1 のフローチャートである。

【図 4 7】 配信サーバ 1 2 と携帯電話機 1 0 7 を用いた配信モードを説明するための第 2 のフローチャートである。

【図 4 8】 メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第 1 のフローチャートである。

【図 4 9】 メモリカード 1 4 0 に保持された暗号化コンテンツデータから、音楽として外部に出力するための再生処理を説明する第 2 のフローチャートである。

【図 5 0】 実施の形態 7 において、2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 1 のフローチャートである。

【図 5 1】 実施の形態 7 において、2 つのメモリカード間において、コンテンツデータおよびキーデータ等の移動または複製を行なう処理を説明するための第 2 のフローチャートである。

【図 5 2】 本発明の実施の形態 8 のコンテンツデータ販売機 3 0 2 0 の構成を示す概略ブロック図である。

【図 5 3】 コンテンツデータ販売機 3 0 2 0 を用いたデータ配信システムにおける配信モードを説明するための第 1 のフローチャートである。

【図 5 4】 コンテンツデータ販売機 3 0 2 0 を用いたデータ配信システム

における配信モードを説明するための第2のフローチャートである。

【図55】 メモリカード140の端子1202部分の構成を説明する概略ブロック図である。

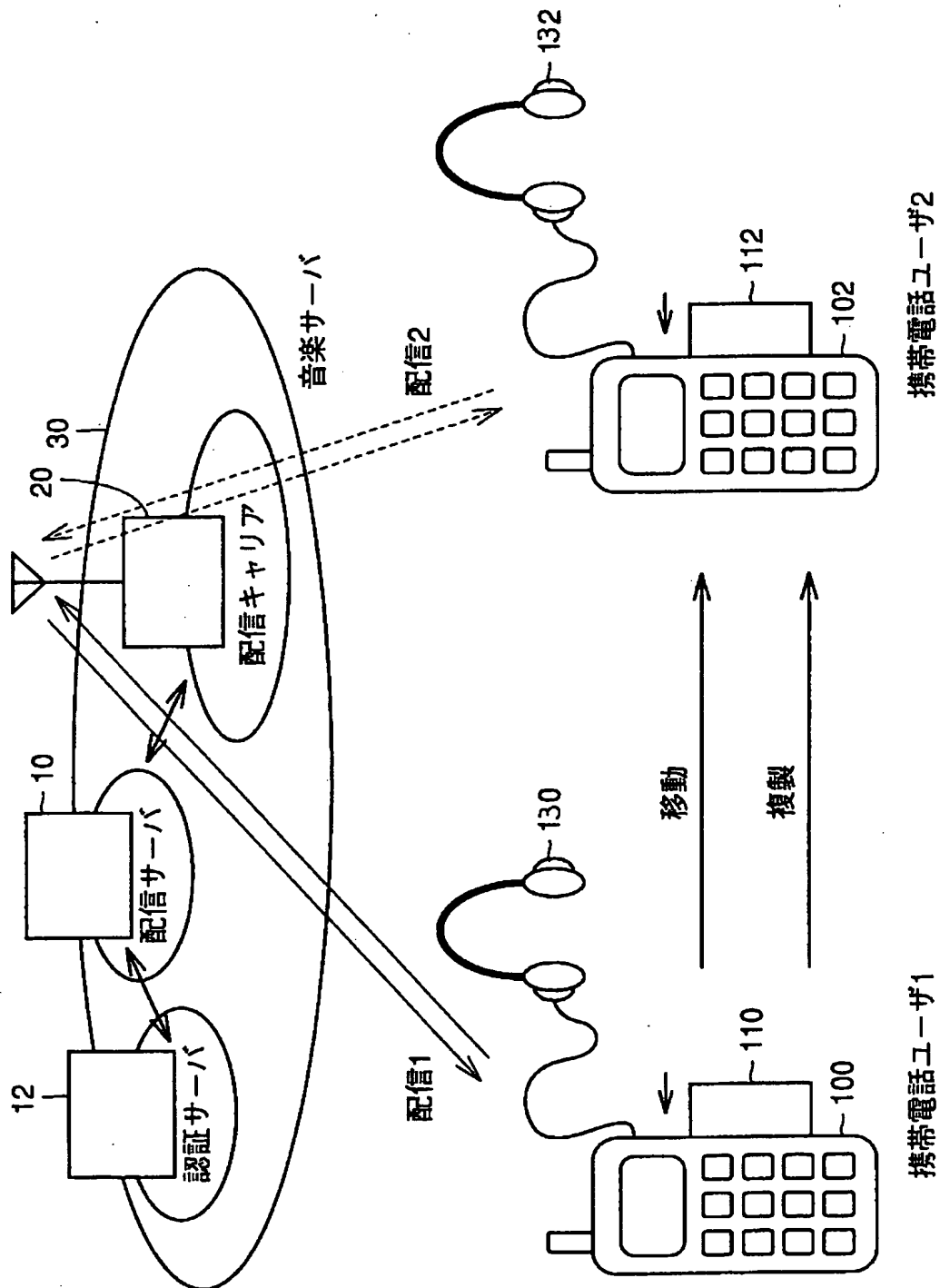
【図56】 メモリカード140の端子1202部分の構成の変形例を説明するための概略ブロック図である。

【符号の説明】

10, 11, 12, 13 配信サーバ、20 配信キャリア、30, 31 音楽サーバ、100, 101, 102, 103, 105, 106, 107 携帯電話機、110, 112, 120, 122, 140, 142 メモリカード、130, 132 ヘッドホン、1102 アンテナ、1104 送受信機、1106 コントローラ、1108 タッチキー部、1110 ディスプレイ、1112 音声再生部、1200 メモリインタフェース、1404 復号処理部、1406 暗号化処理部、1408, 1409 切替スイッチ、1410 復号処理部、1412 メモリ、1414 暗号化処理部、1416 復号処理部、1420 コントローラ、1430 暗号化処理部、1432 セッションキー発生部、1434, 1435 切替スイッチ、1502 セッションキー発生部、1504 暗号化処理部、1506 復号処理部、1508 音楽再生部、1510 混合部、1512 デジタルアナログ変換器、1525 [KPp、Crtf] KPmaster保持部、2000, 3000, 3010 コンテンツデータ販売機。

【書類名】 図面

【図 1】

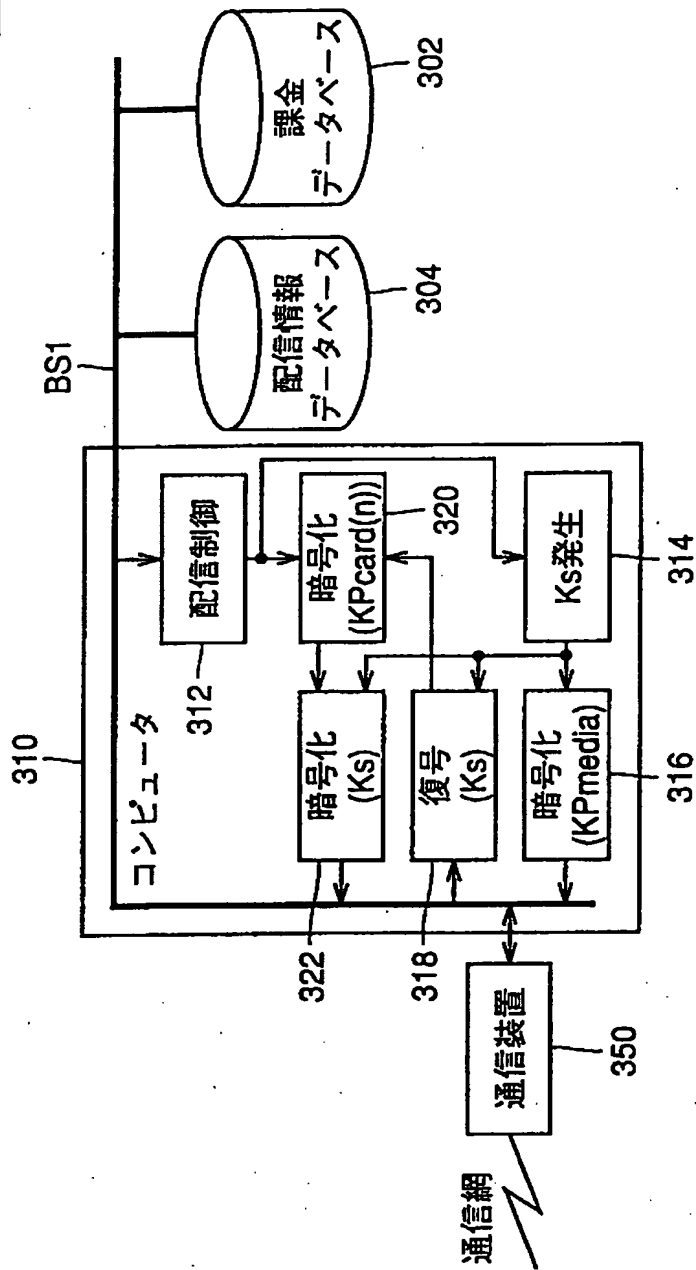


【図 2】

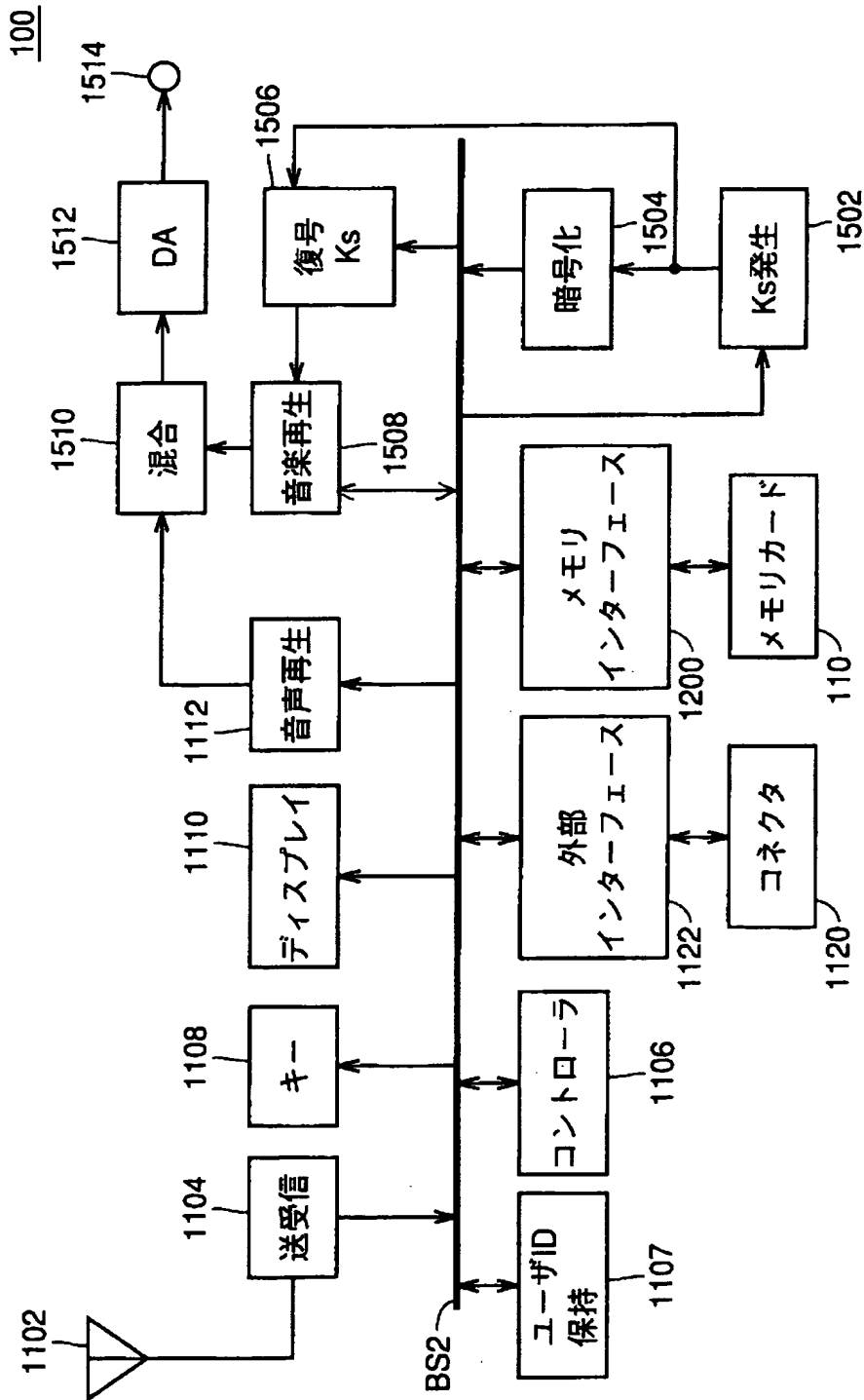
	記号	属性	特性	
			媒体固有	メモリカードの種類ごとに固有な情報を有する
メモリカード内 管理の鍵	Kmedia(n)	秘密復号鍵		メモリカード毎に異なる
	Kcard(n)	秘密復号鍵		Kcard(n)と対を成す。
	KPcard(n)	公開暗号化鍵		KPcard(n)により暗号化されたデータは、Kcard(n)で復号可能
メモリカード外 管理の鍵	KPmedia(n)	公開暗号化鍵	媒体固有	Kmediaと対を成す。 KPmediaにより暗号化されたデータは、Kmediaで復号可能。
	Ks	共通鍵	セッション 固有	通信毎 (例: アクセス毎) に発生。 配信サーバ、携帯電話機にて管理
配信データ	Kc	共通鍵	ライセン スキー	暗号化コンテンツデータの復号鍵
	License-ID	再生に関する 情報		例: 曲目の特定情報 再生回数の制限情報
	User-ID	受信者を識別 する情報		例: 電話番号
	Dc	コンテンツ データ		例: 音楽
	[Dc]Kc	暗号化コン テンツデータ		共通鍵Kcにより暗号化されたコン テンツデータ

【図 3】

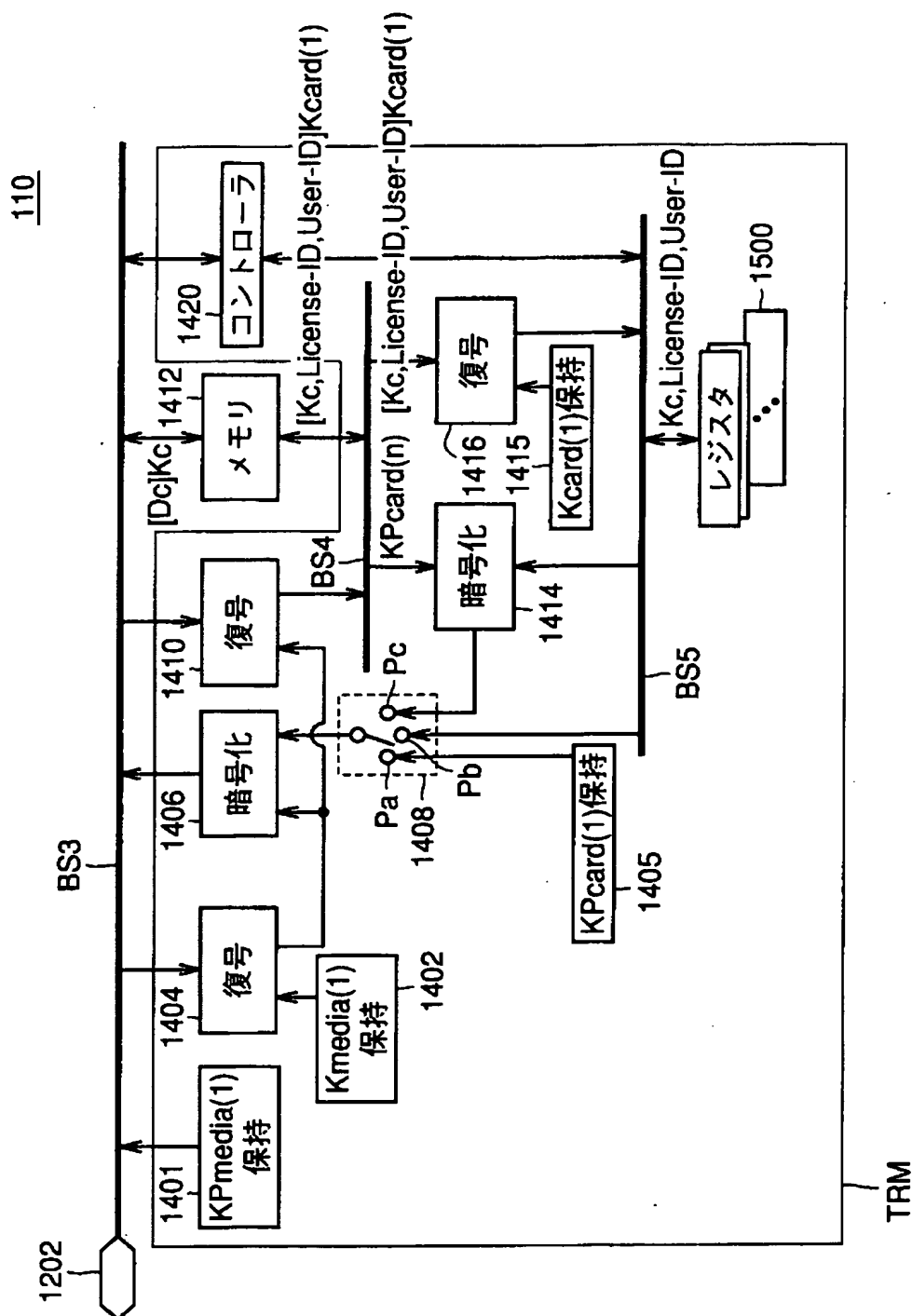
10



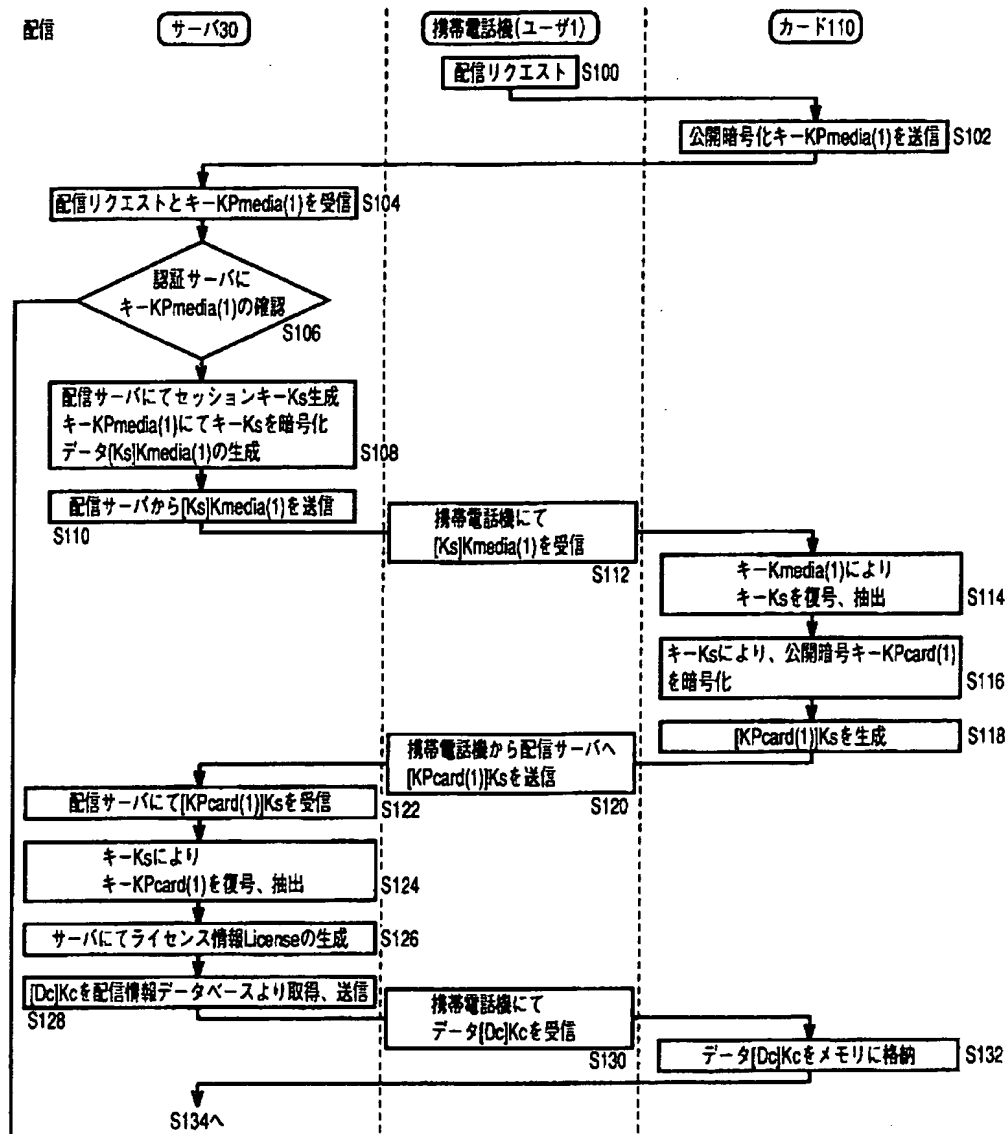
【図 4】



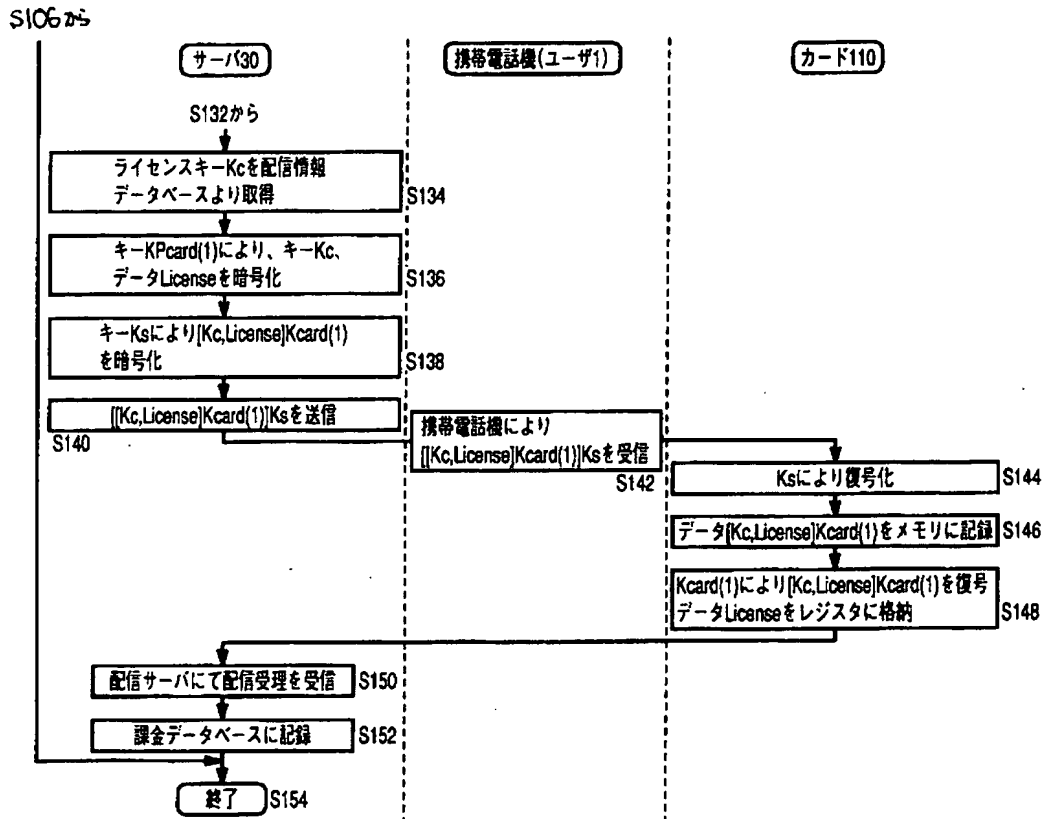
【図 5】



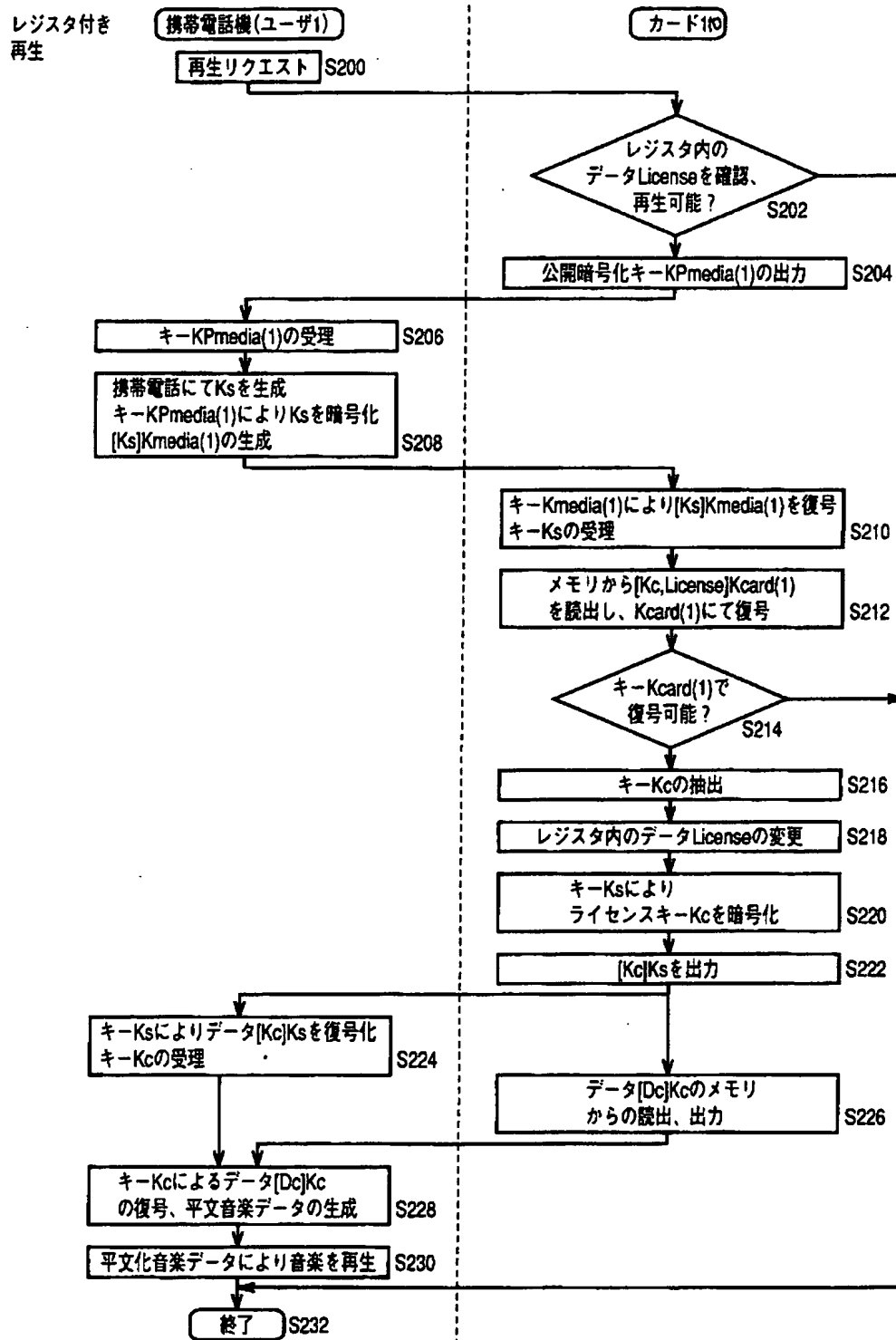
【図 6】



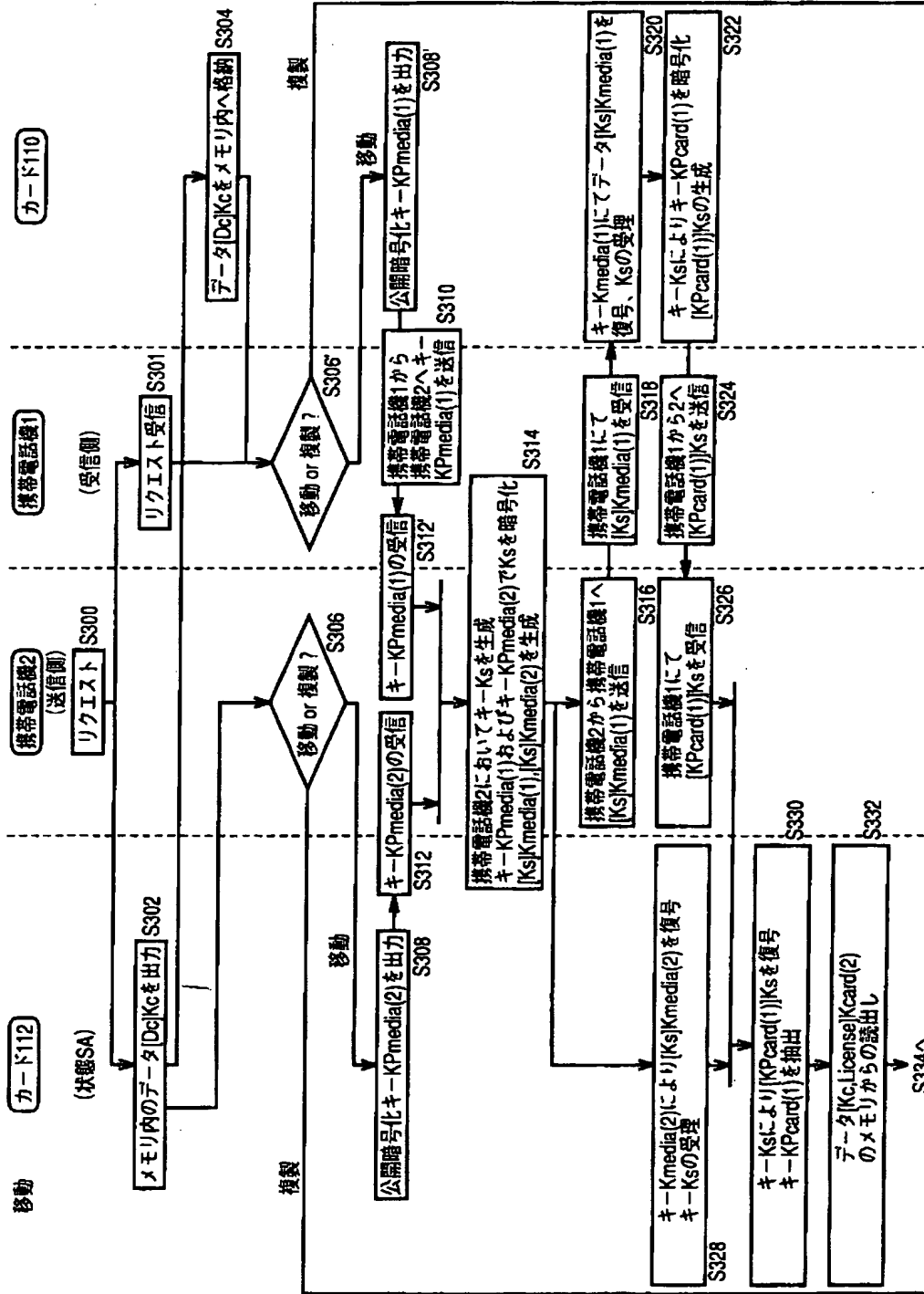
【図 7】



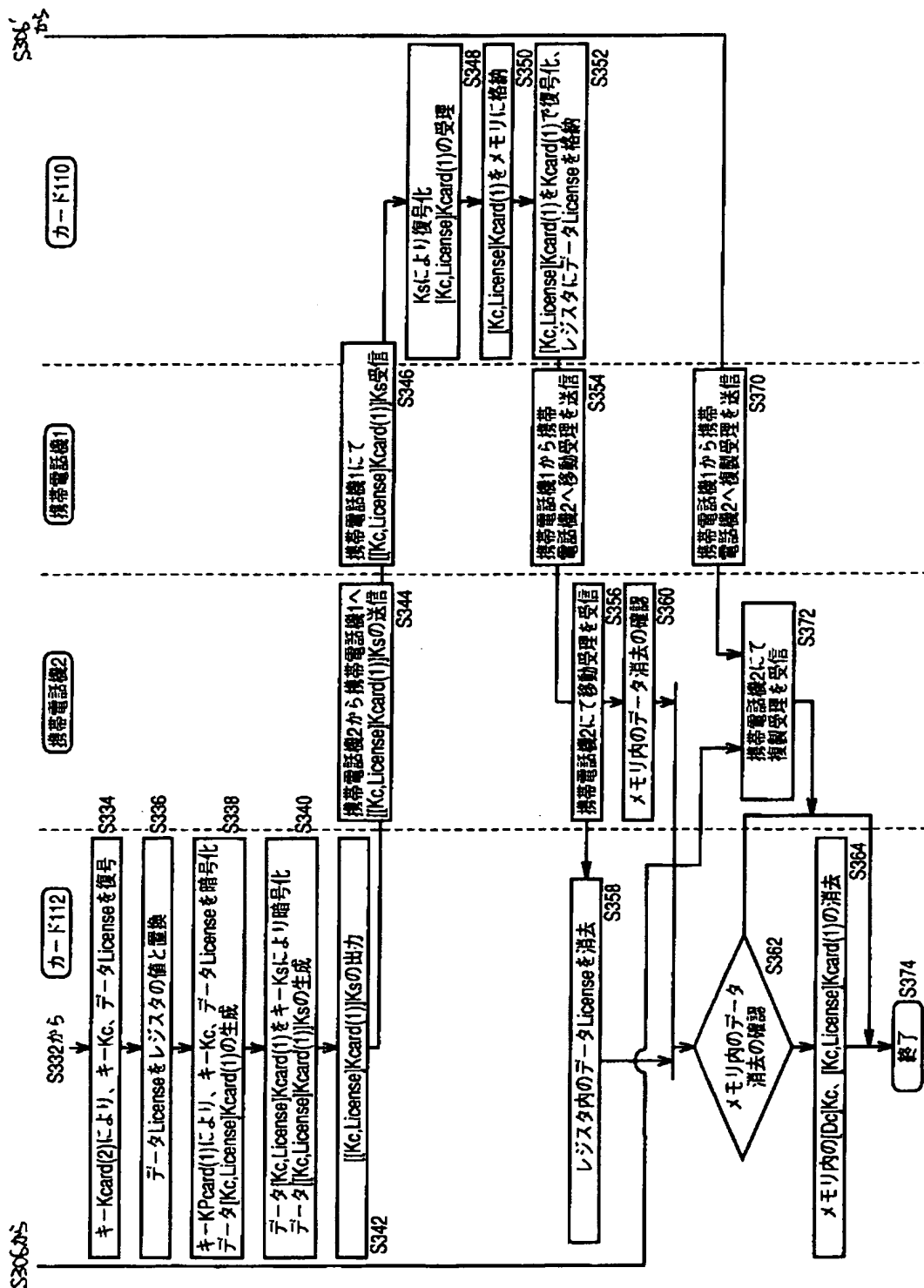
【図 8】



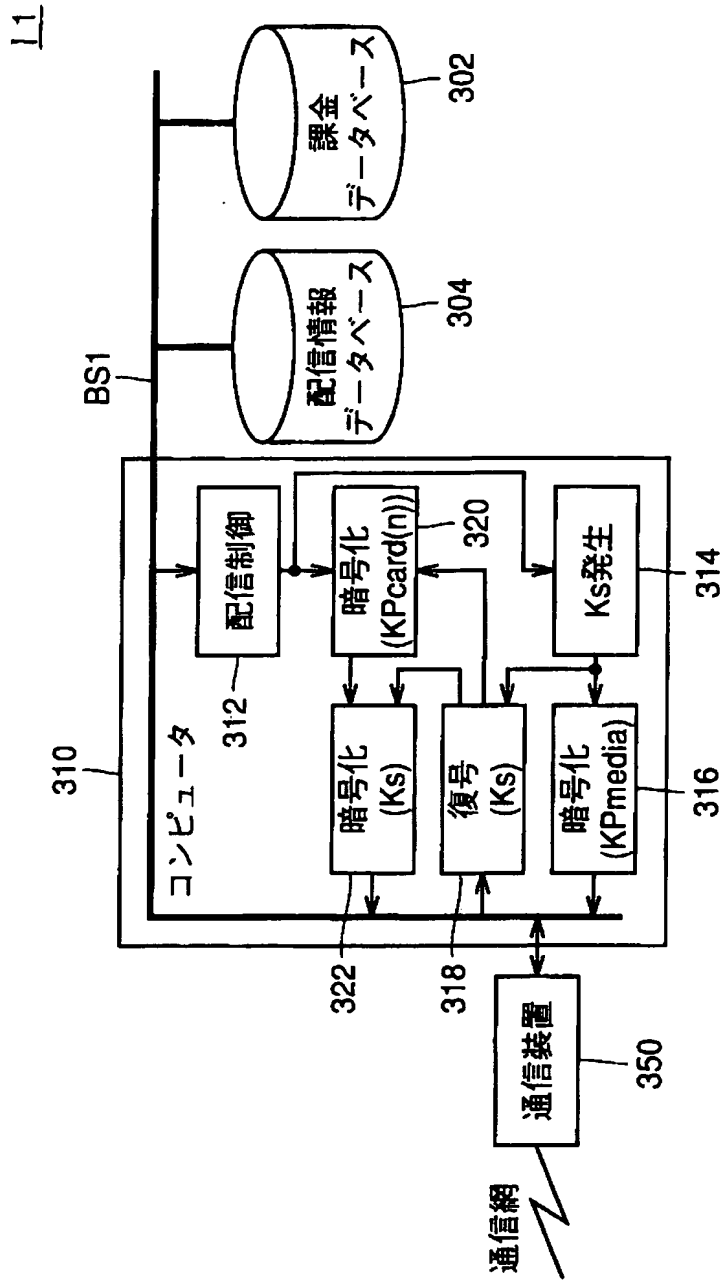
【図 9】



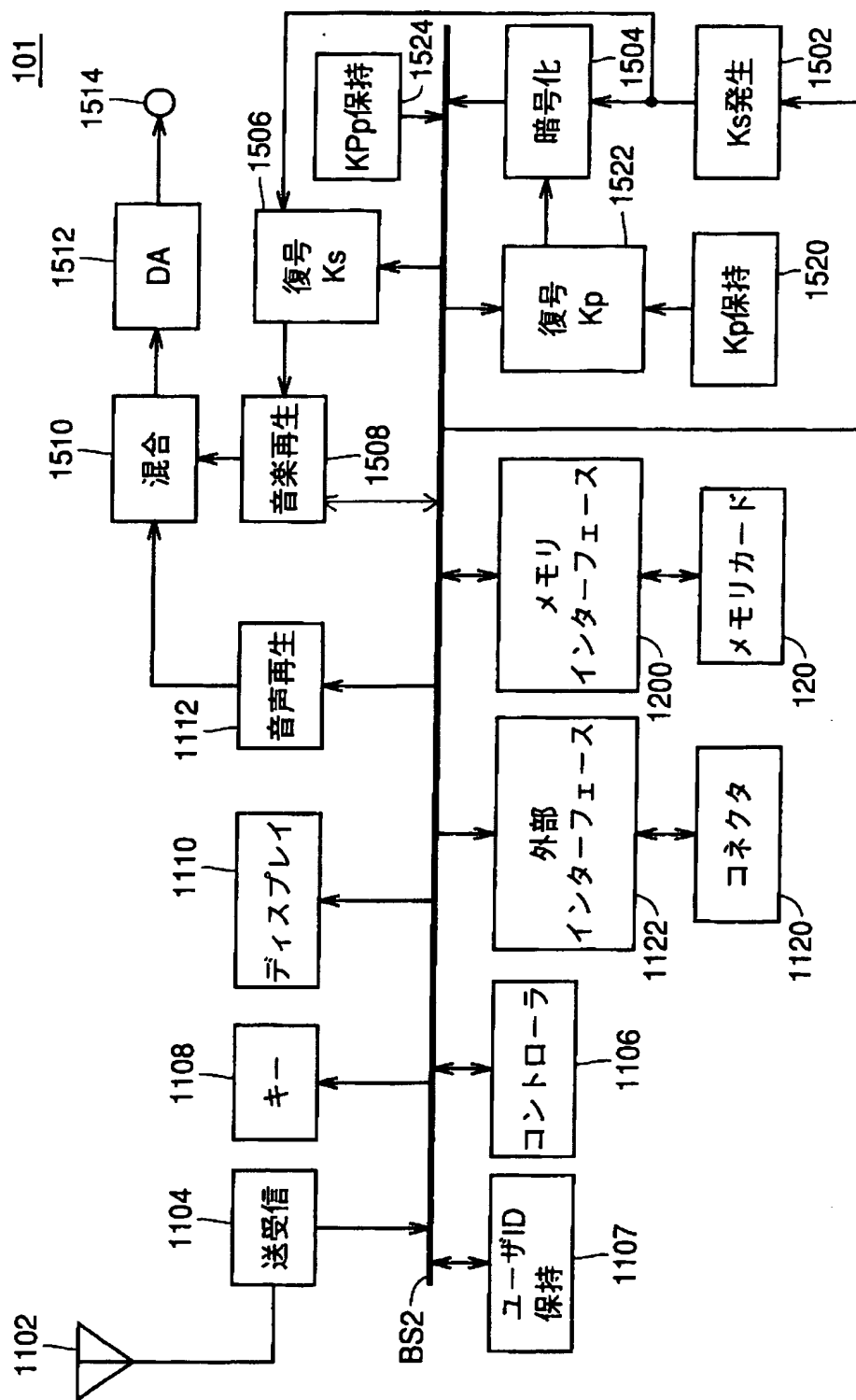
【図 10】



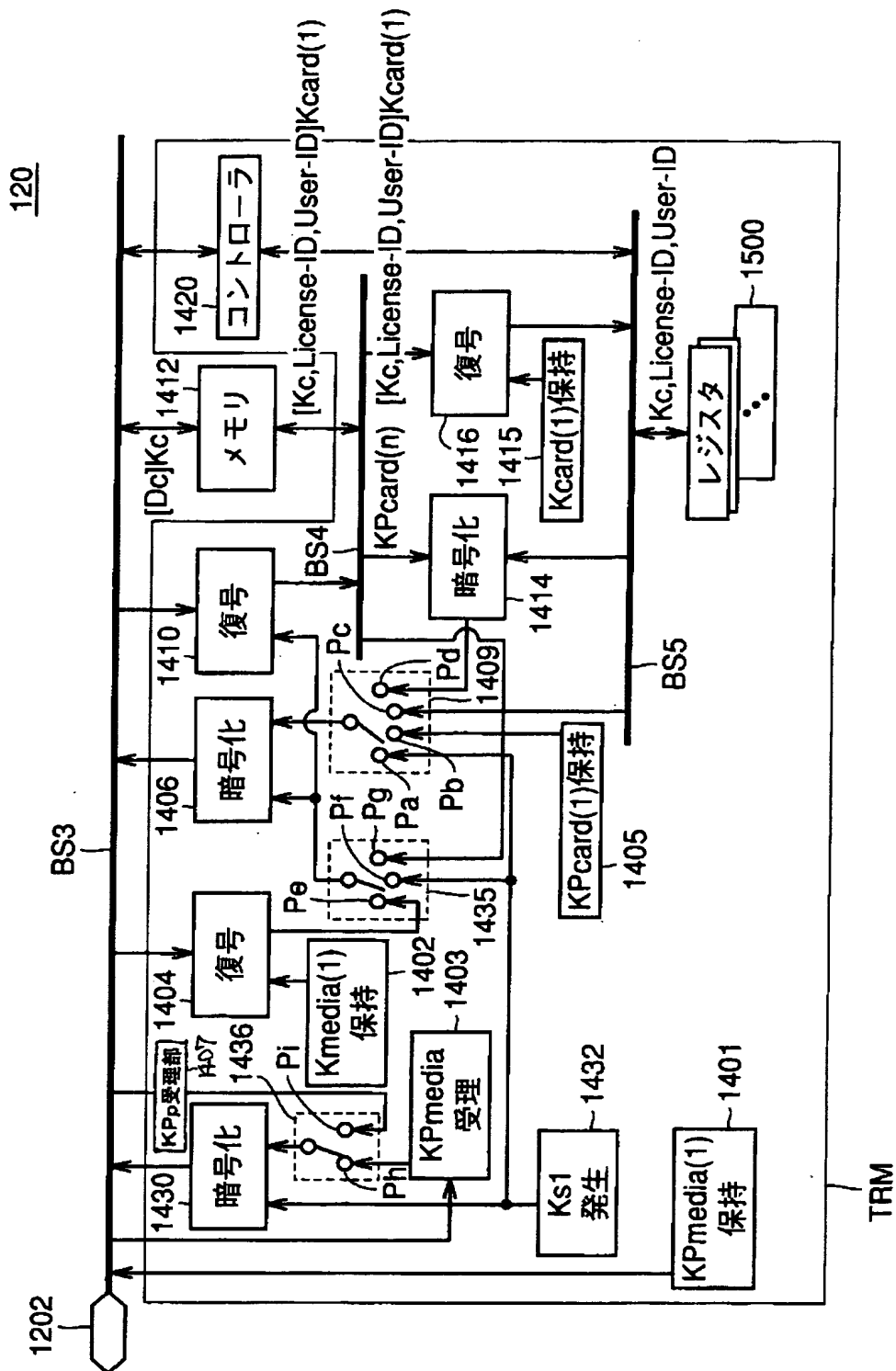
【図 1 1】



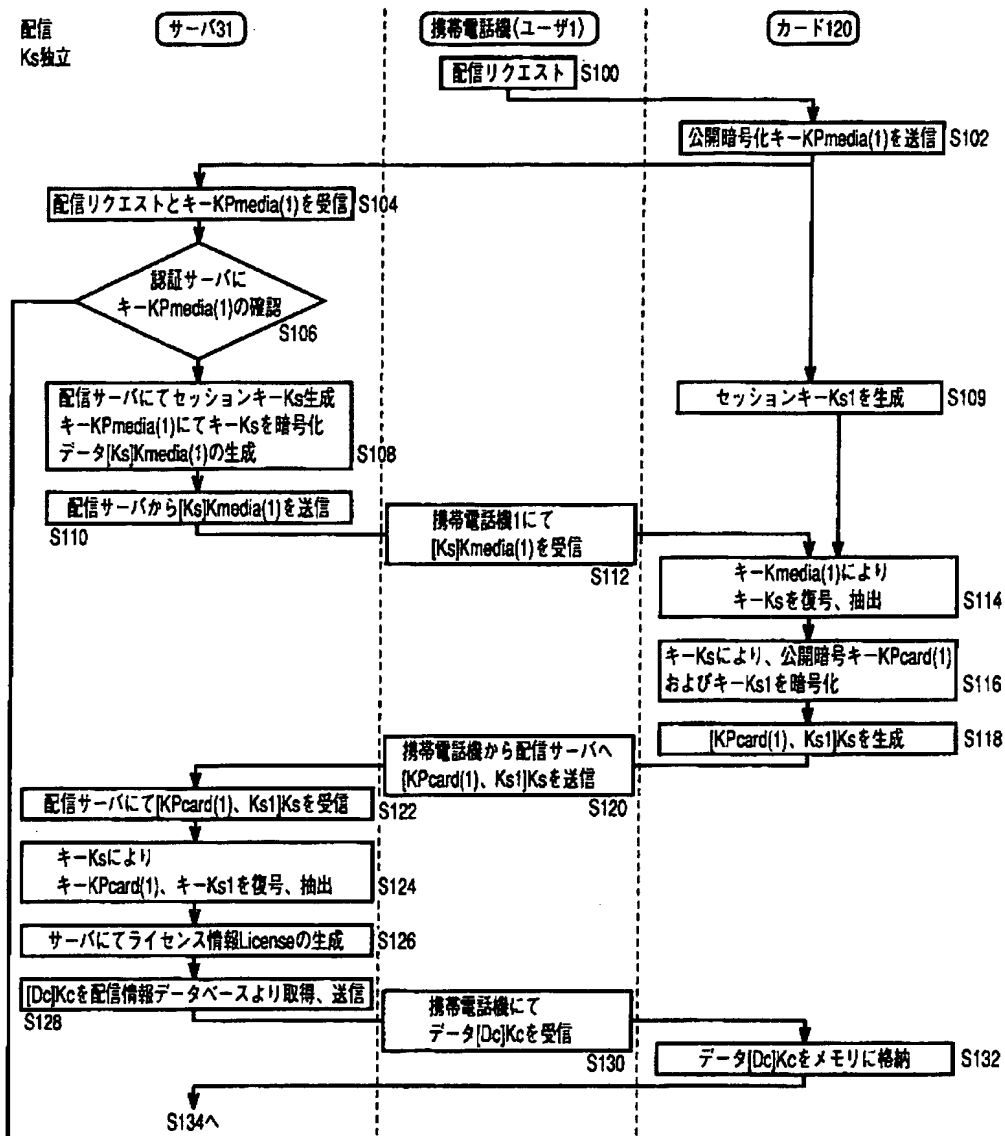
【図 1 2】



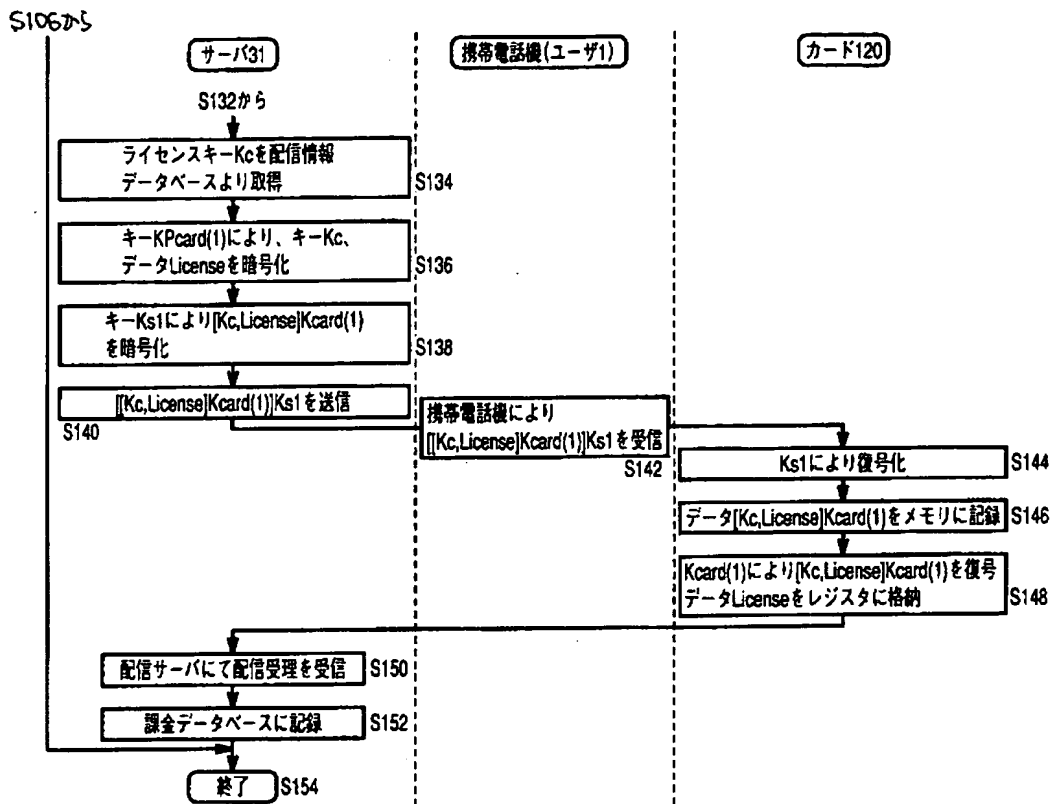
【図 13】



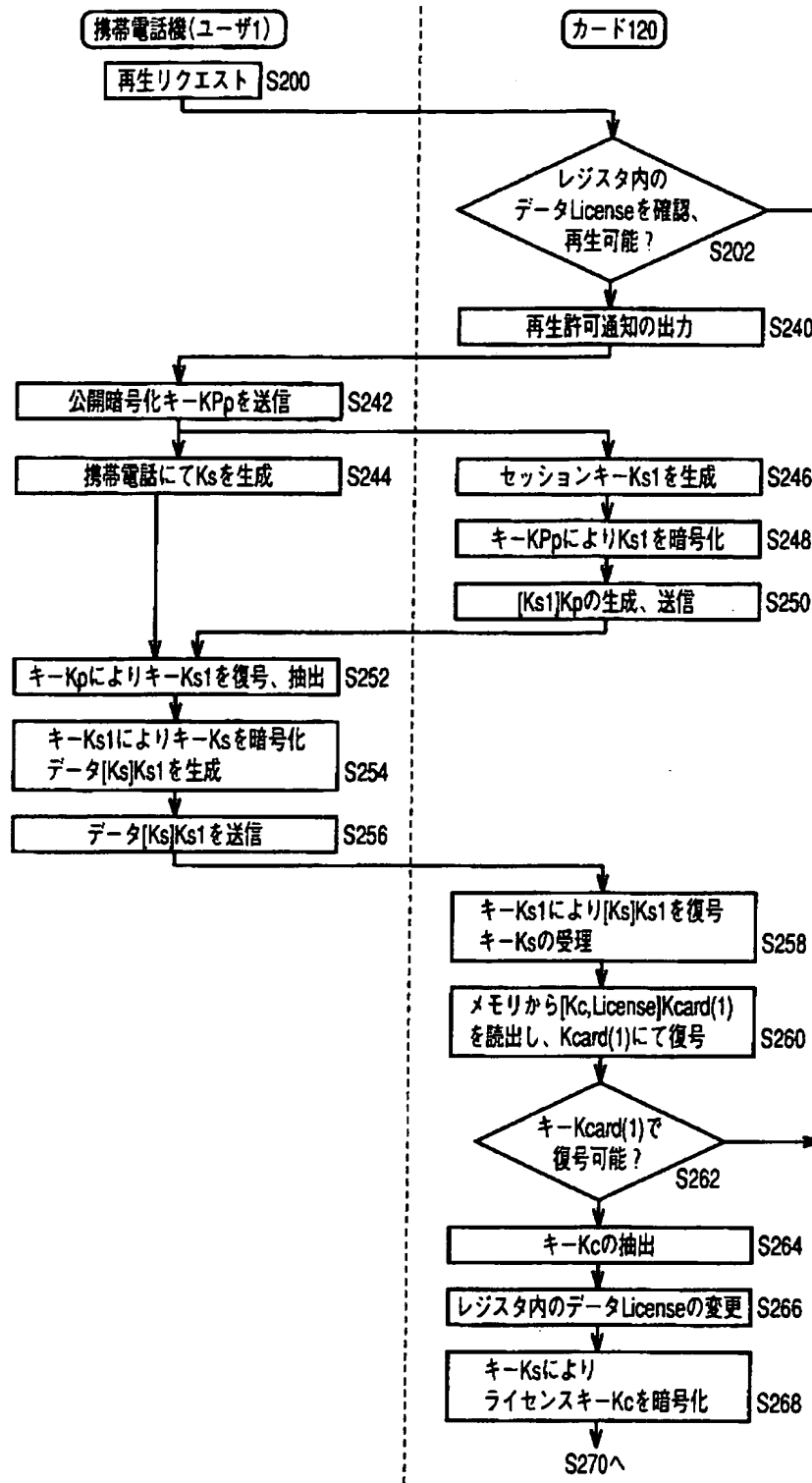
【図 1 4】



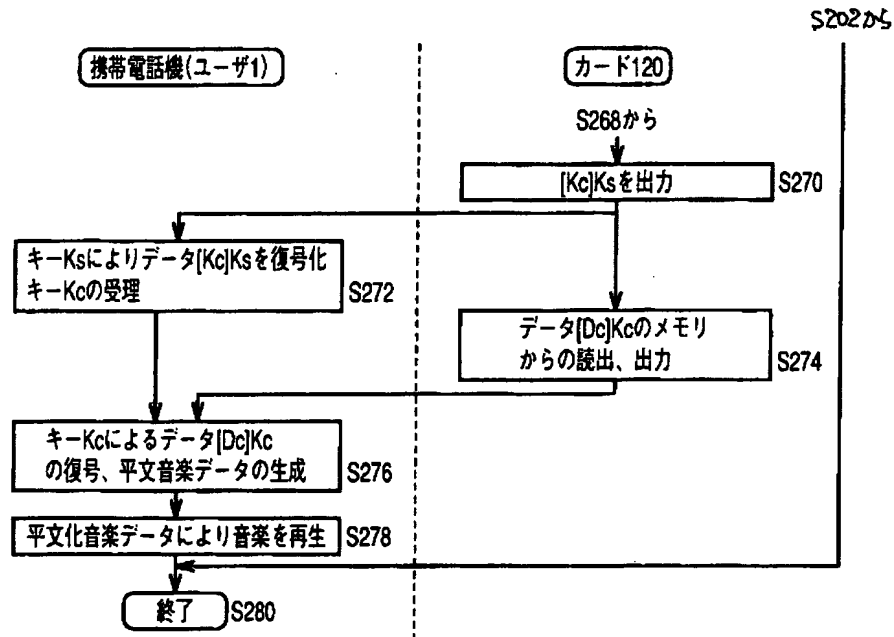
【図 1 5】



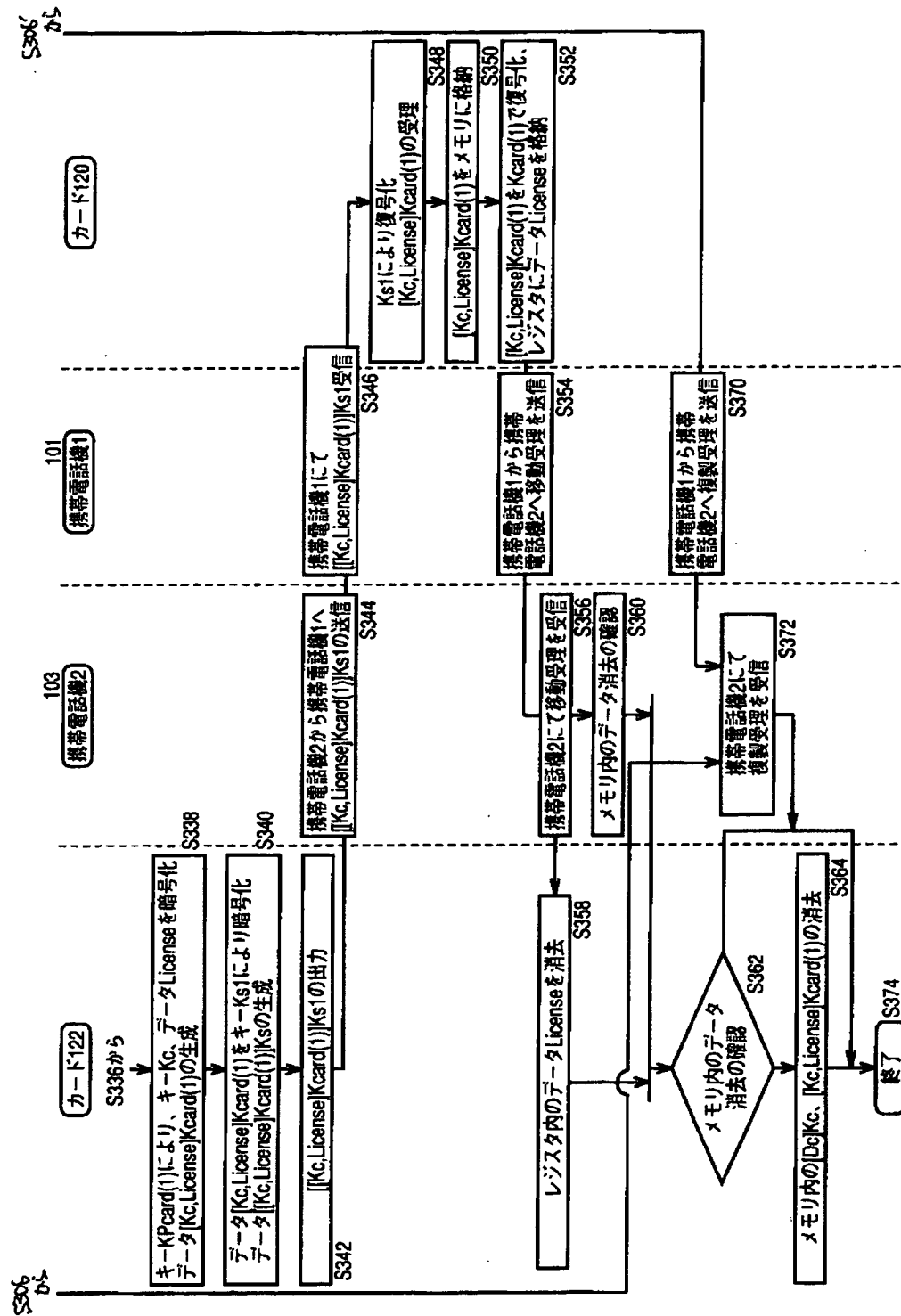
【図 1 6】

再生
Ks独立

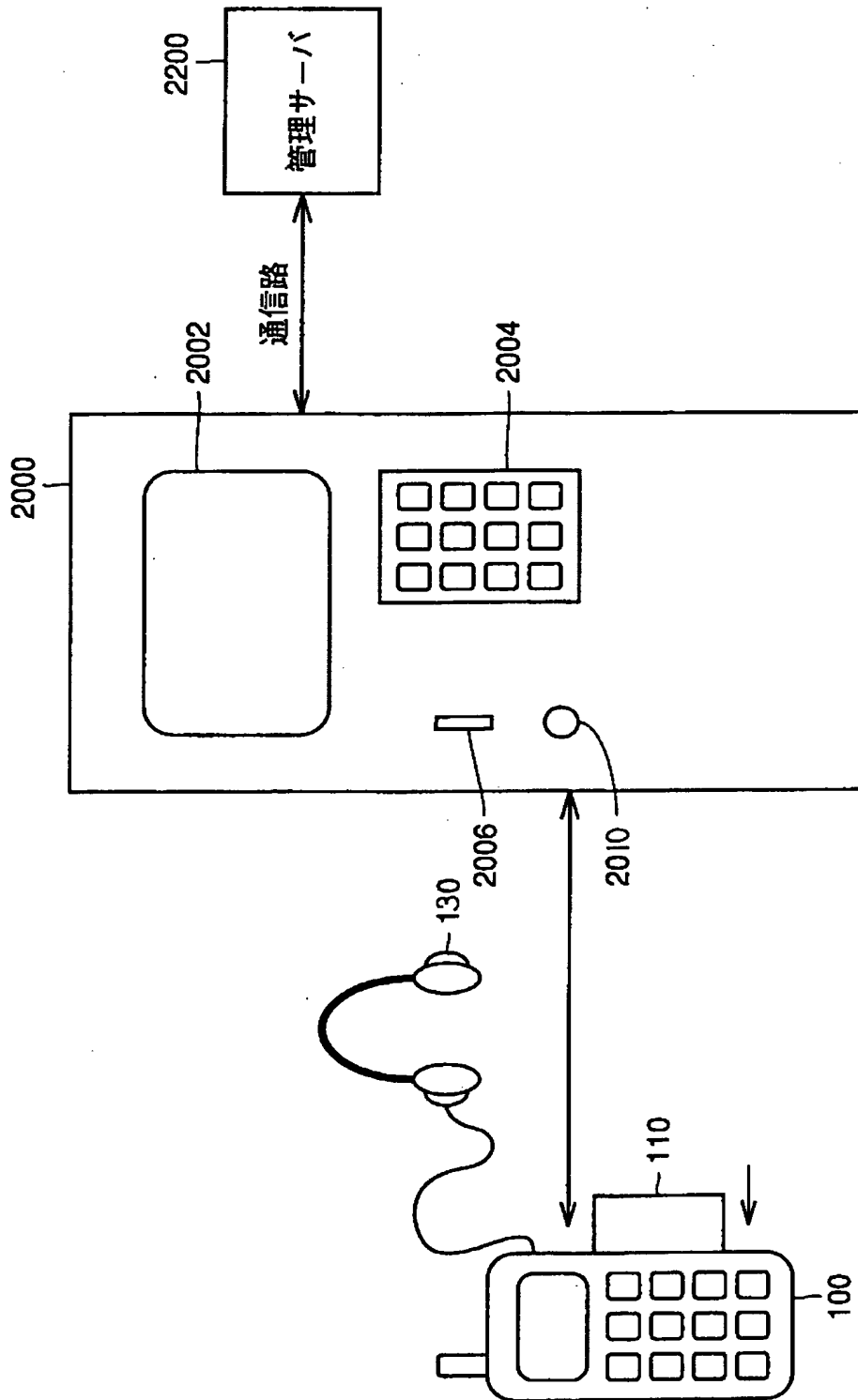
【図 1 7】



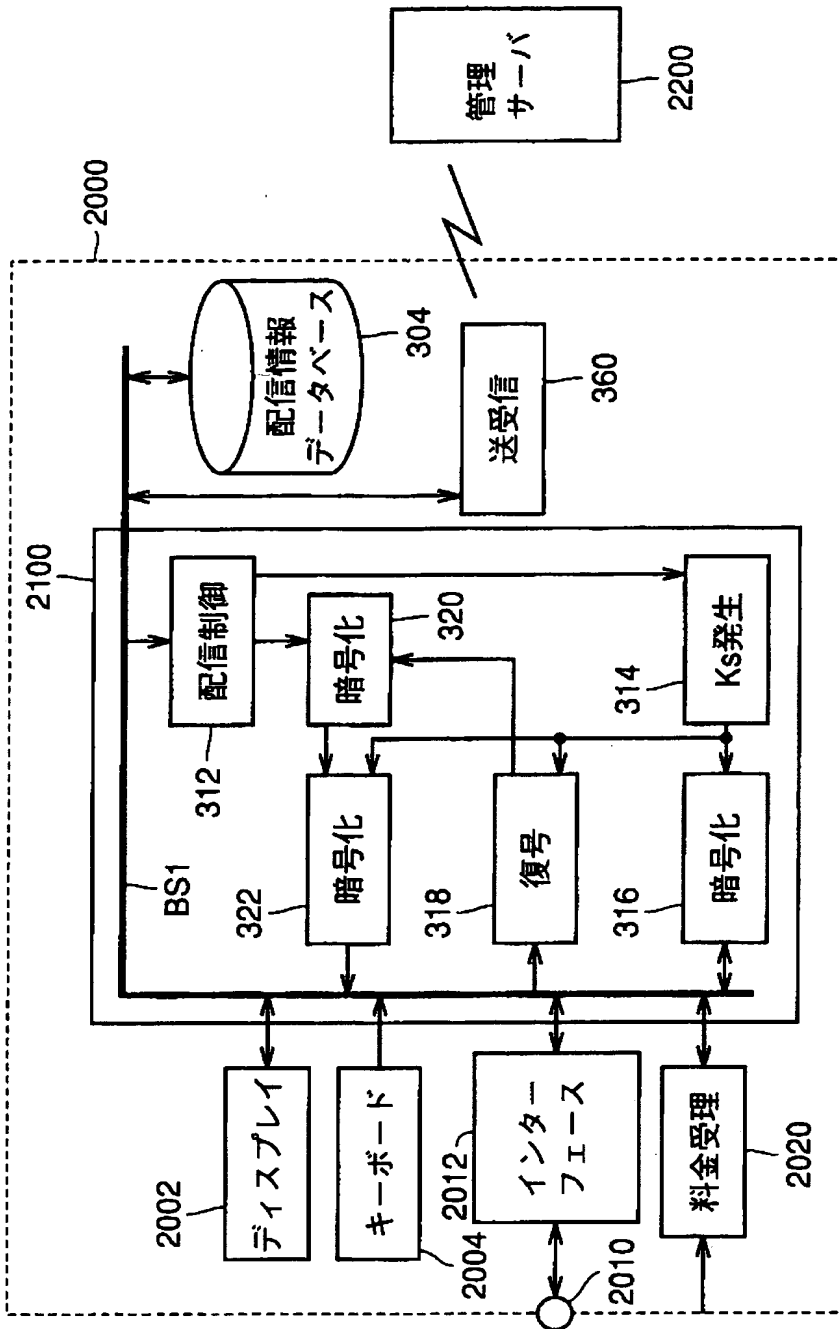
【図 1 9】



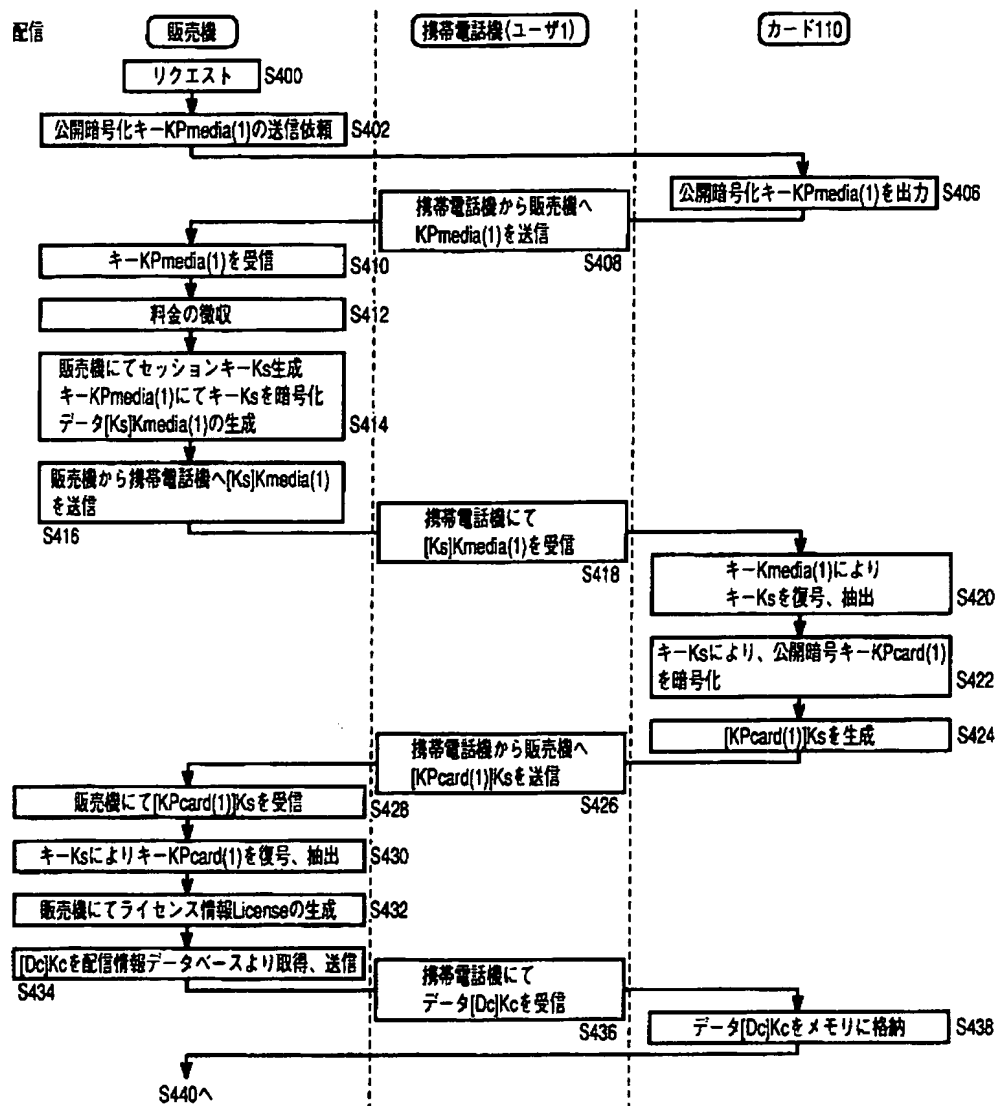
【図 2 0】



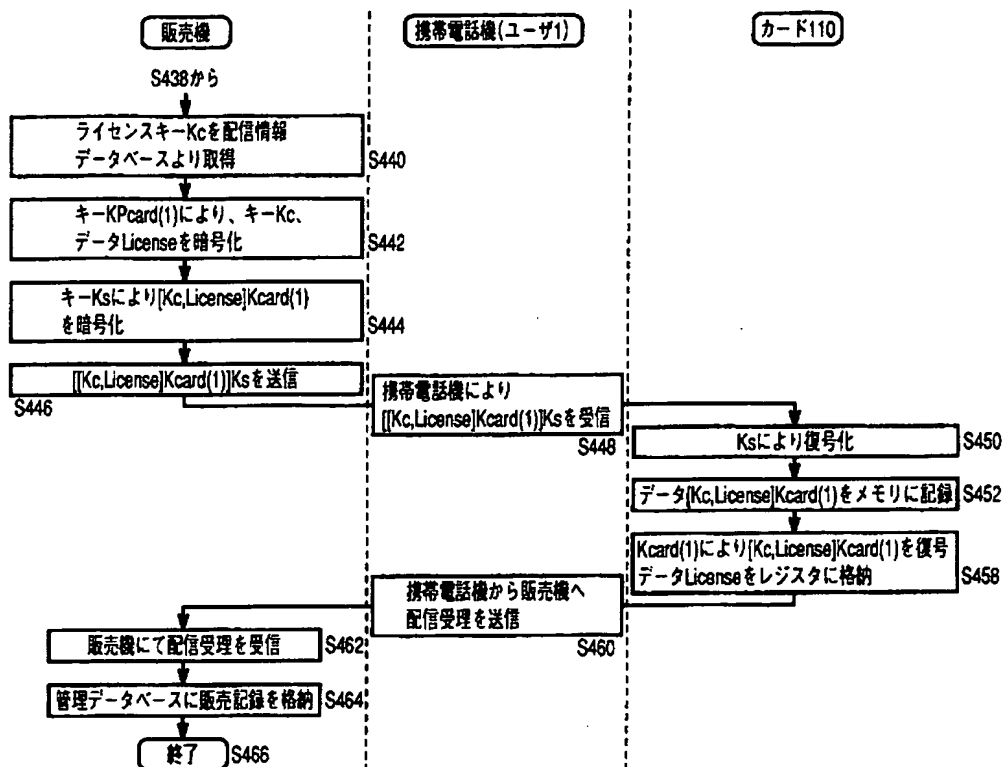
【図 2 1】



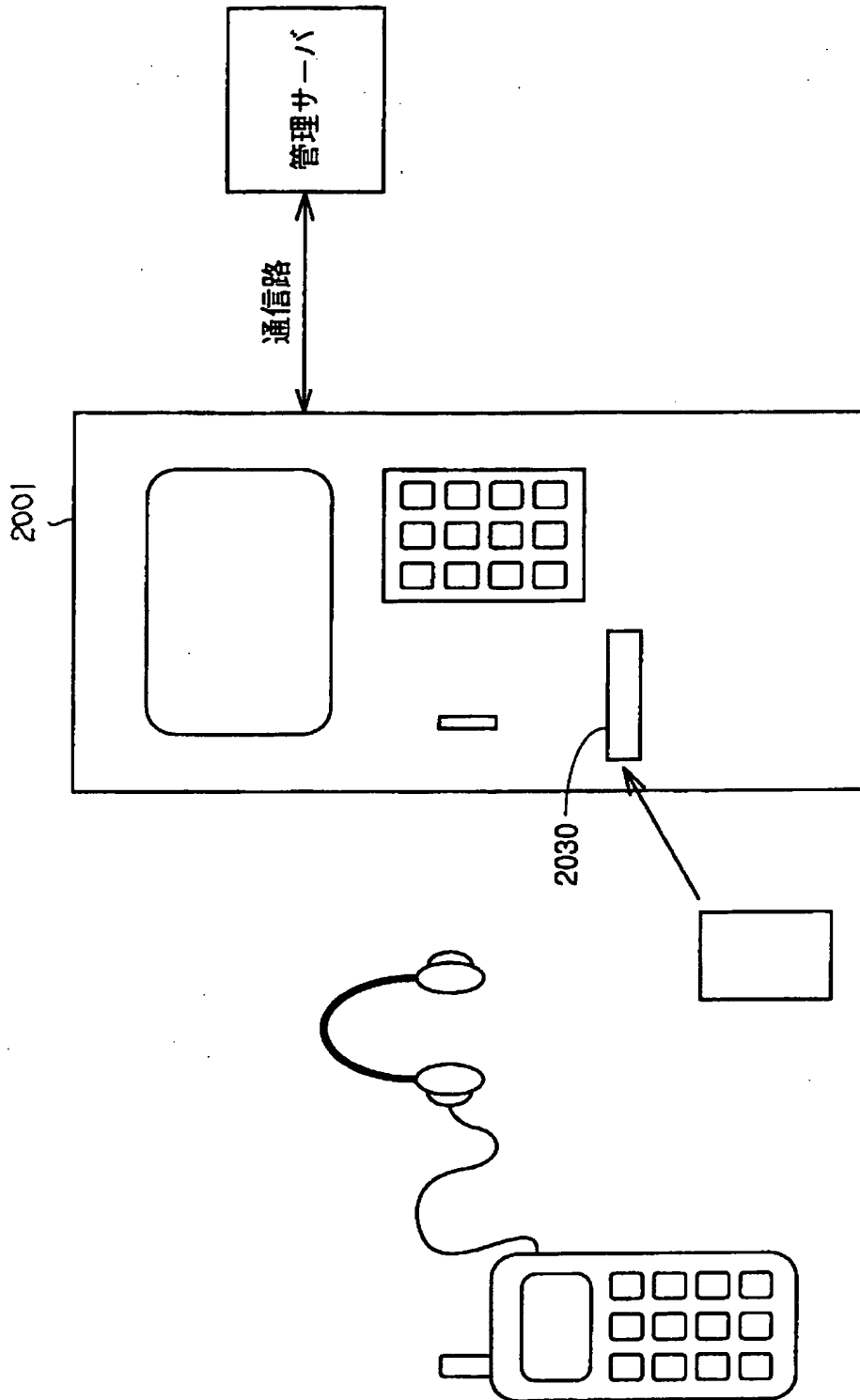
【図 2 2】



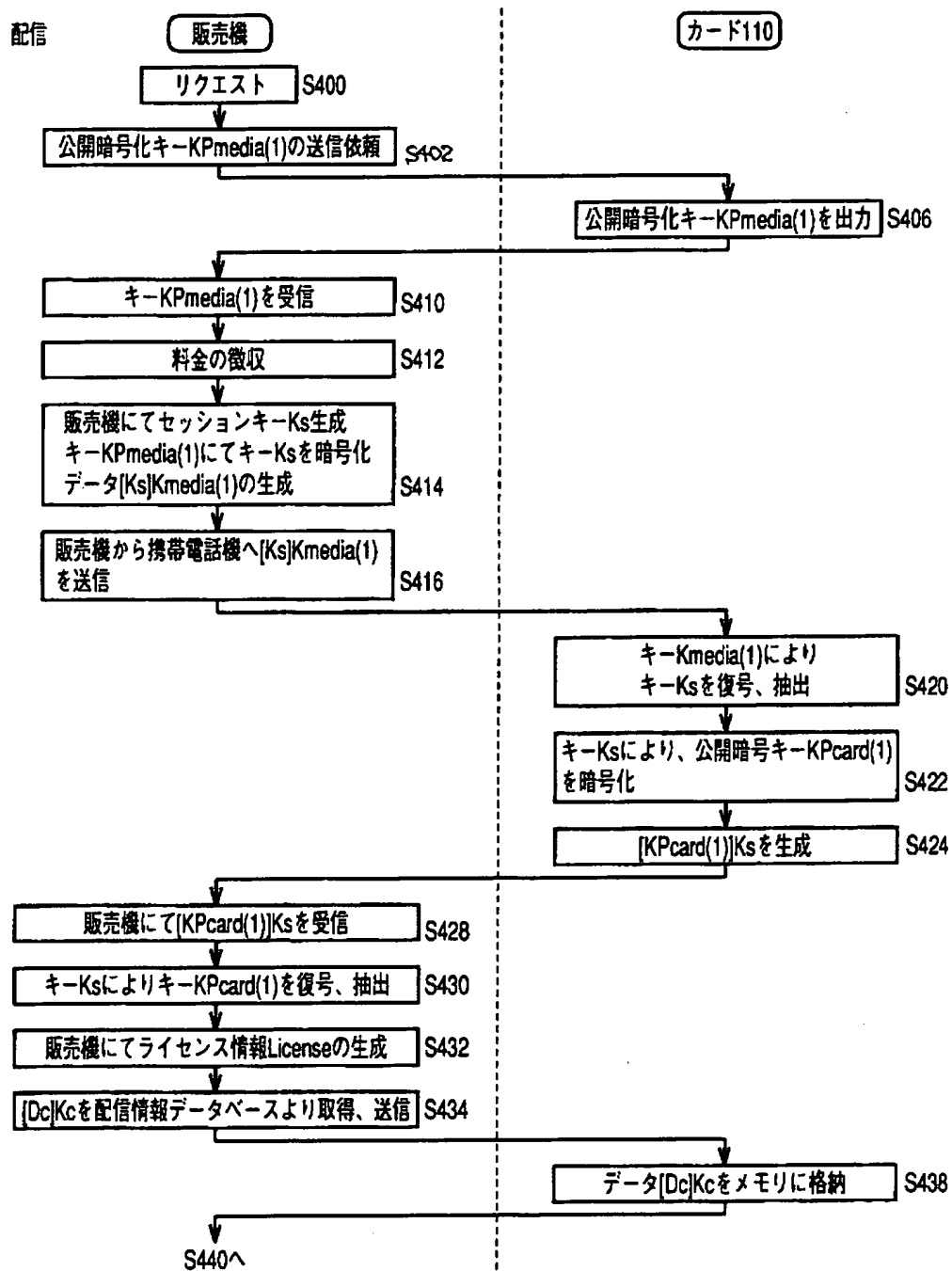
【図 2 3】



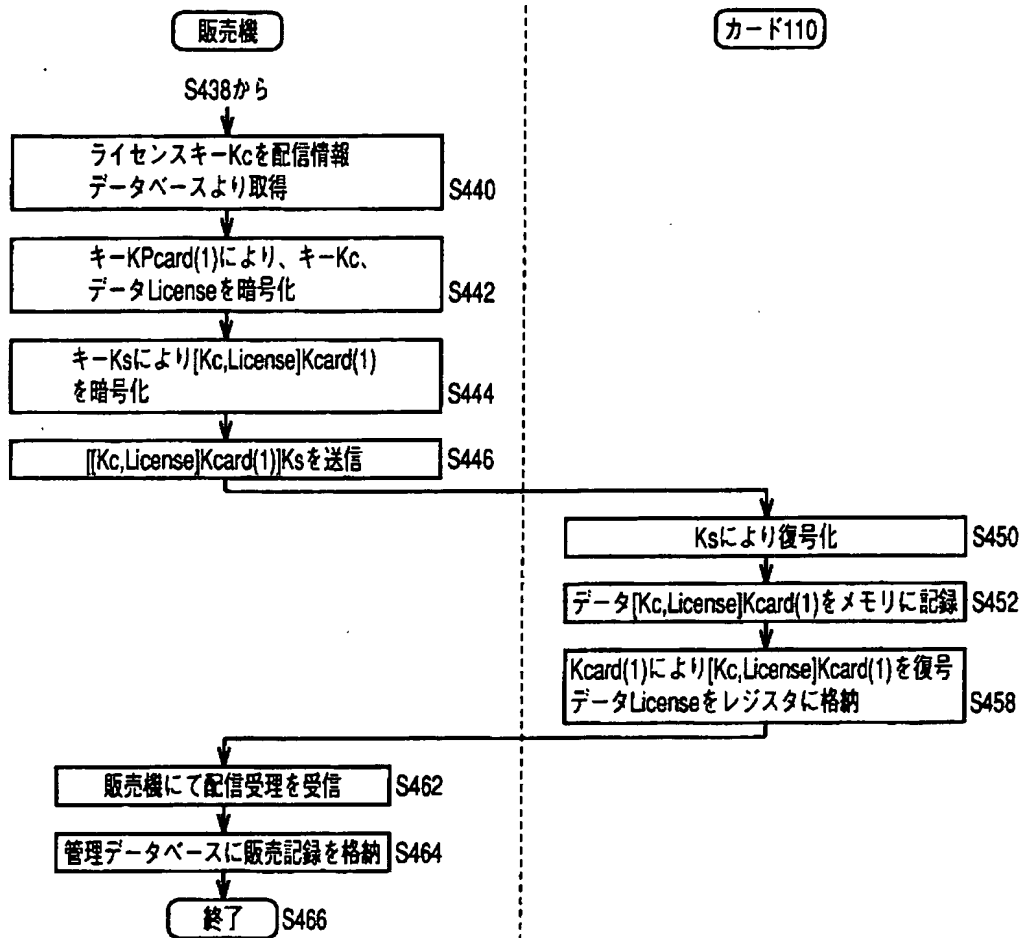
【図 2 4】



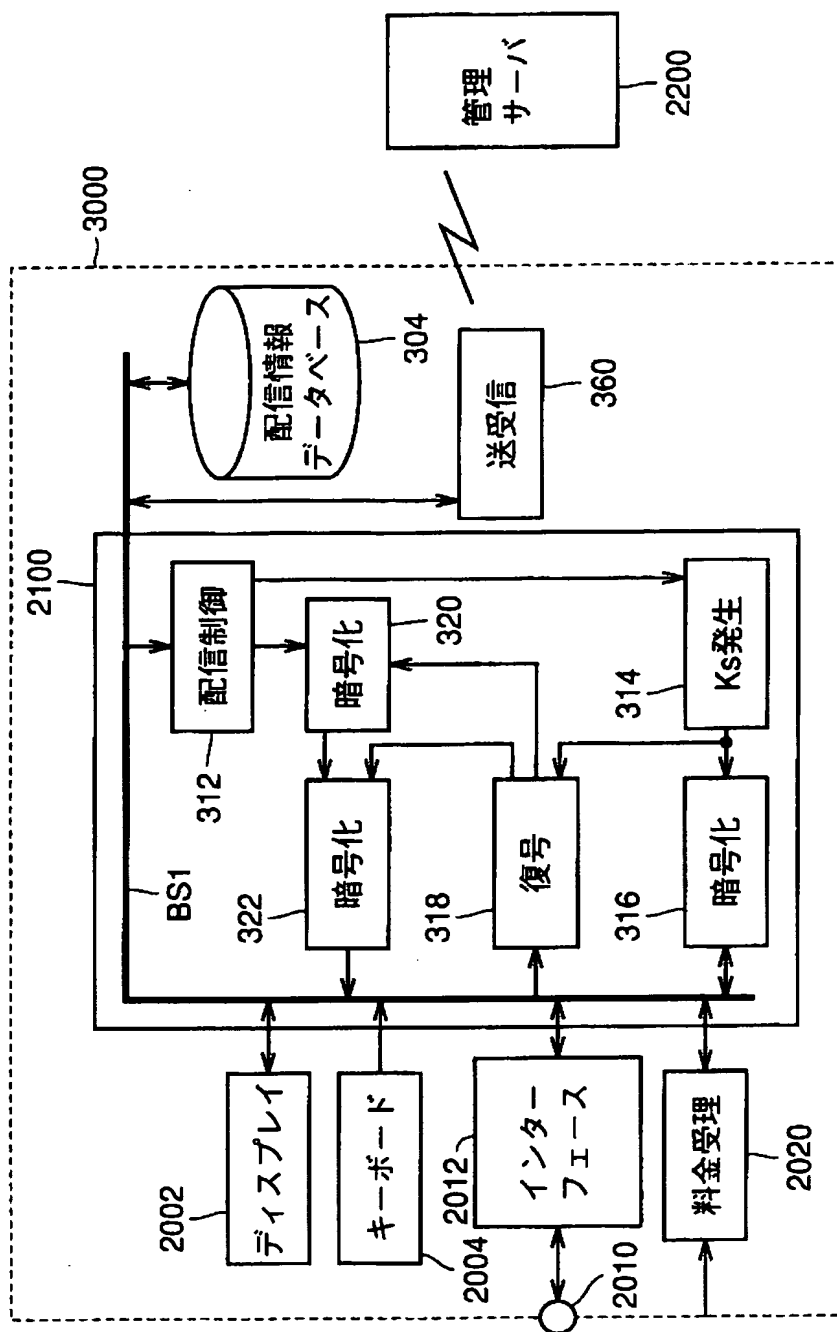
【図 2 5】



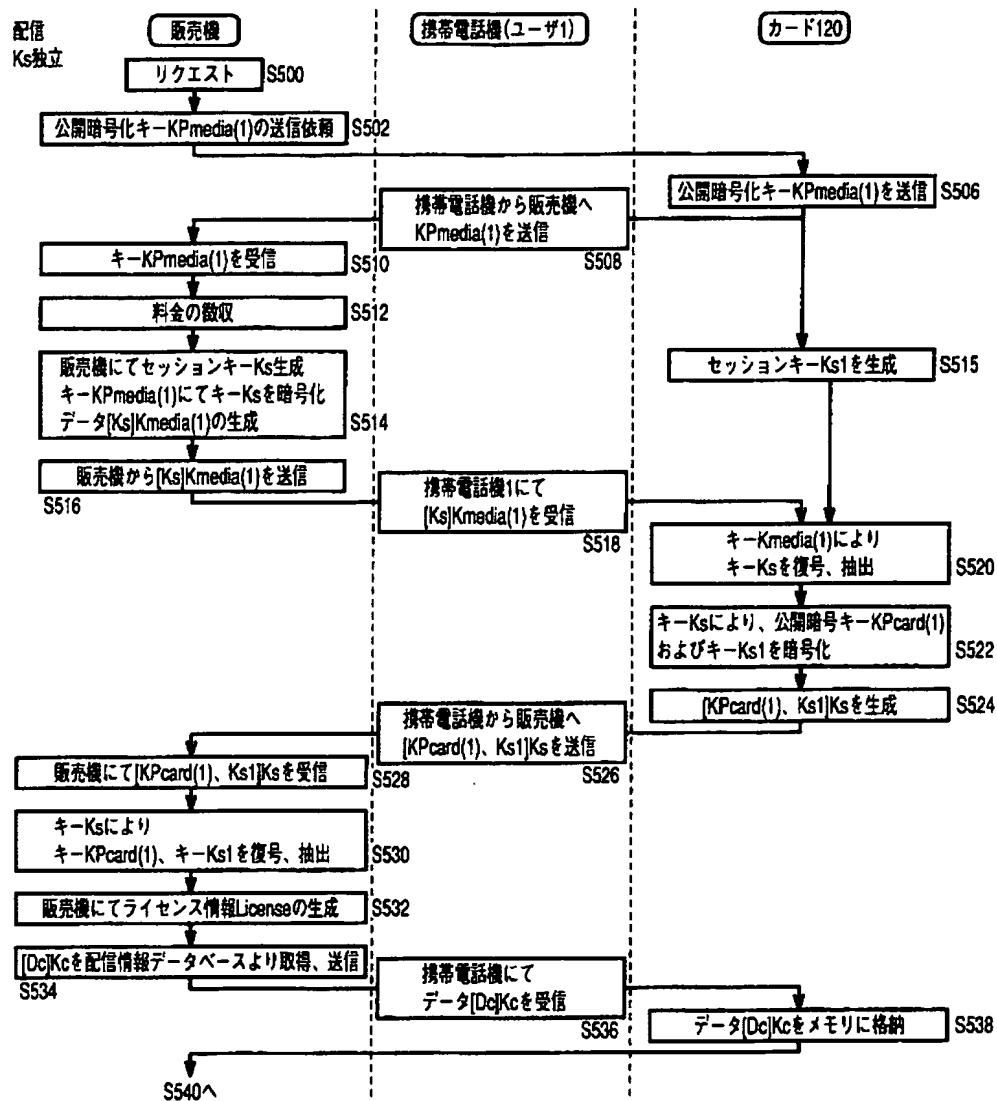
【図 2 6】



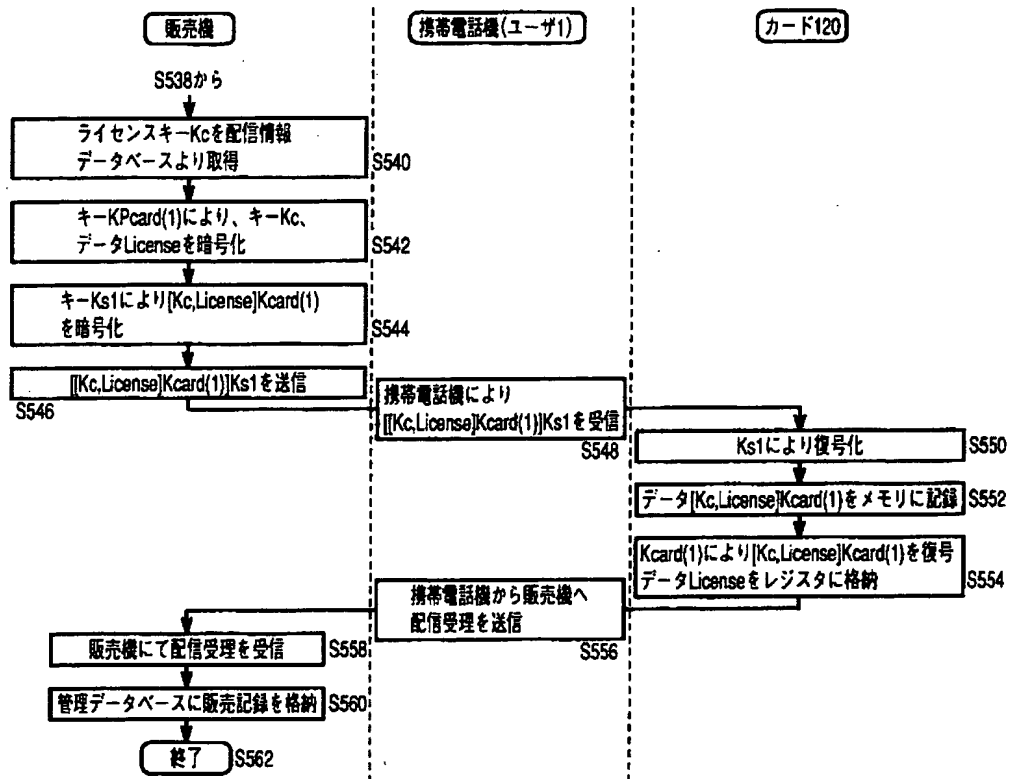
【図 2 7】



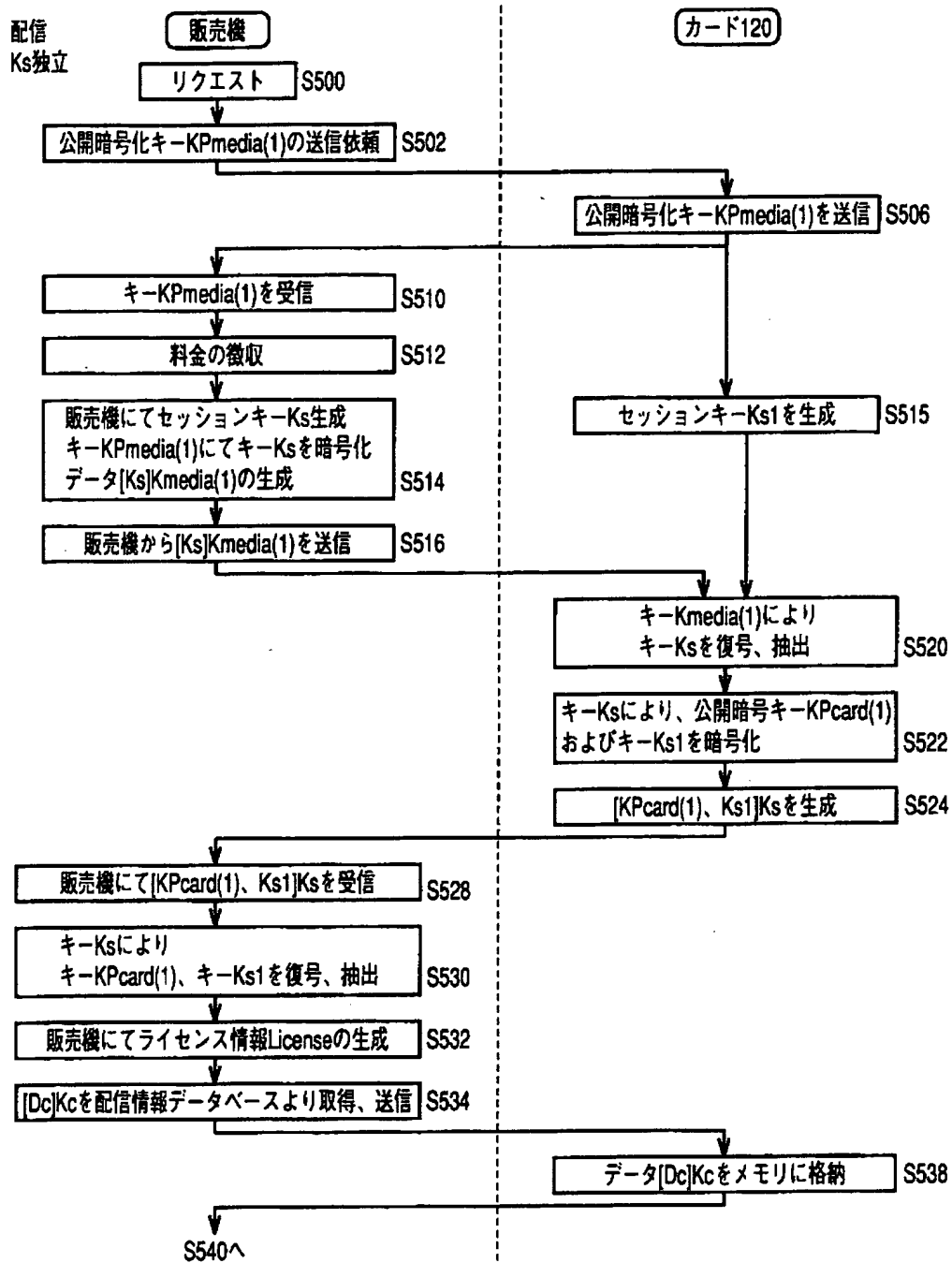
【図 2 8】



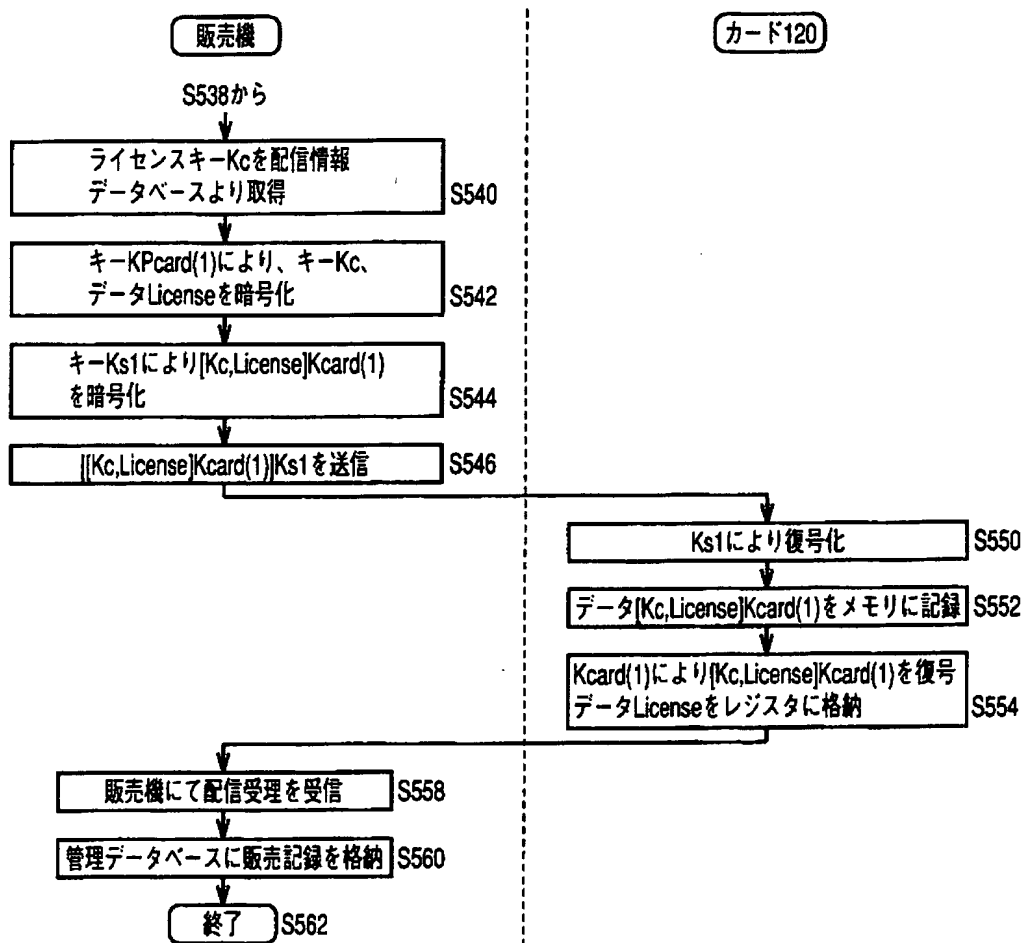
【図 2 9】



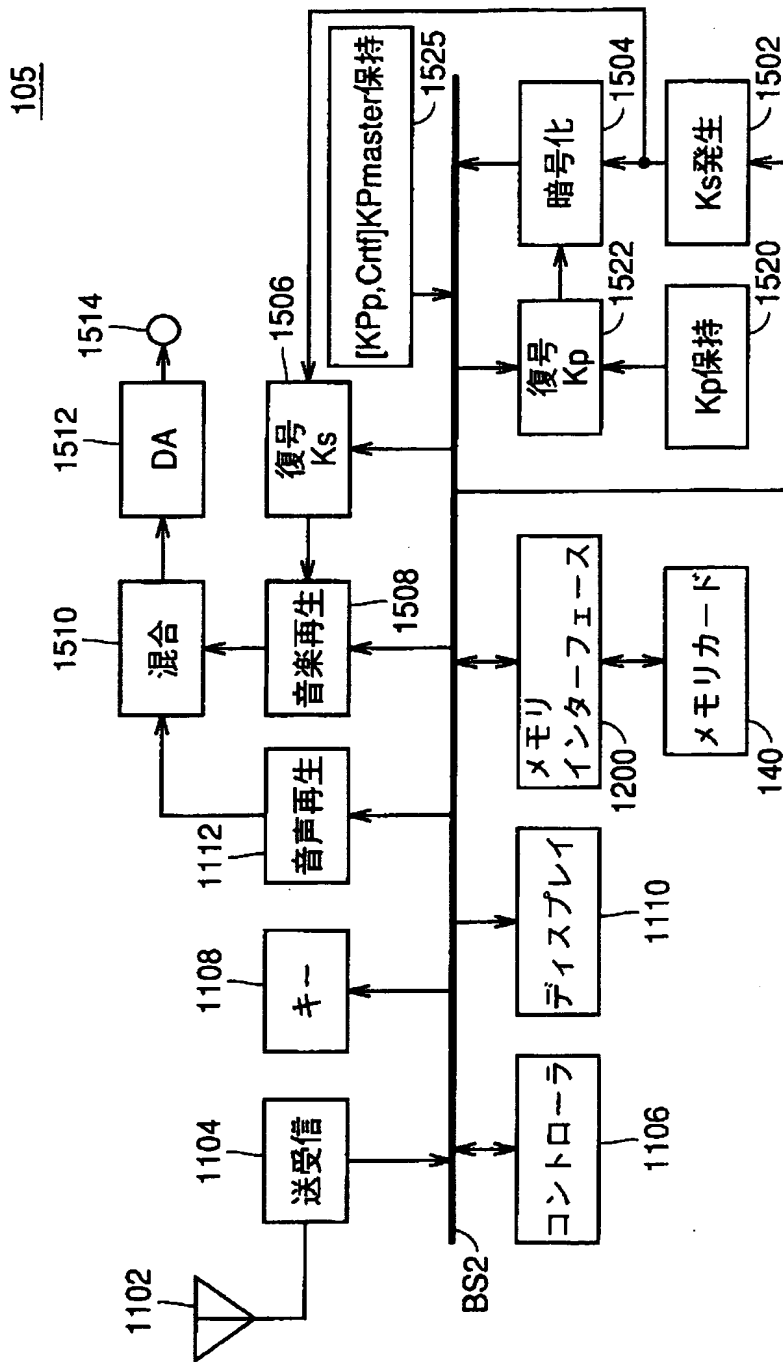
【図 3 0】



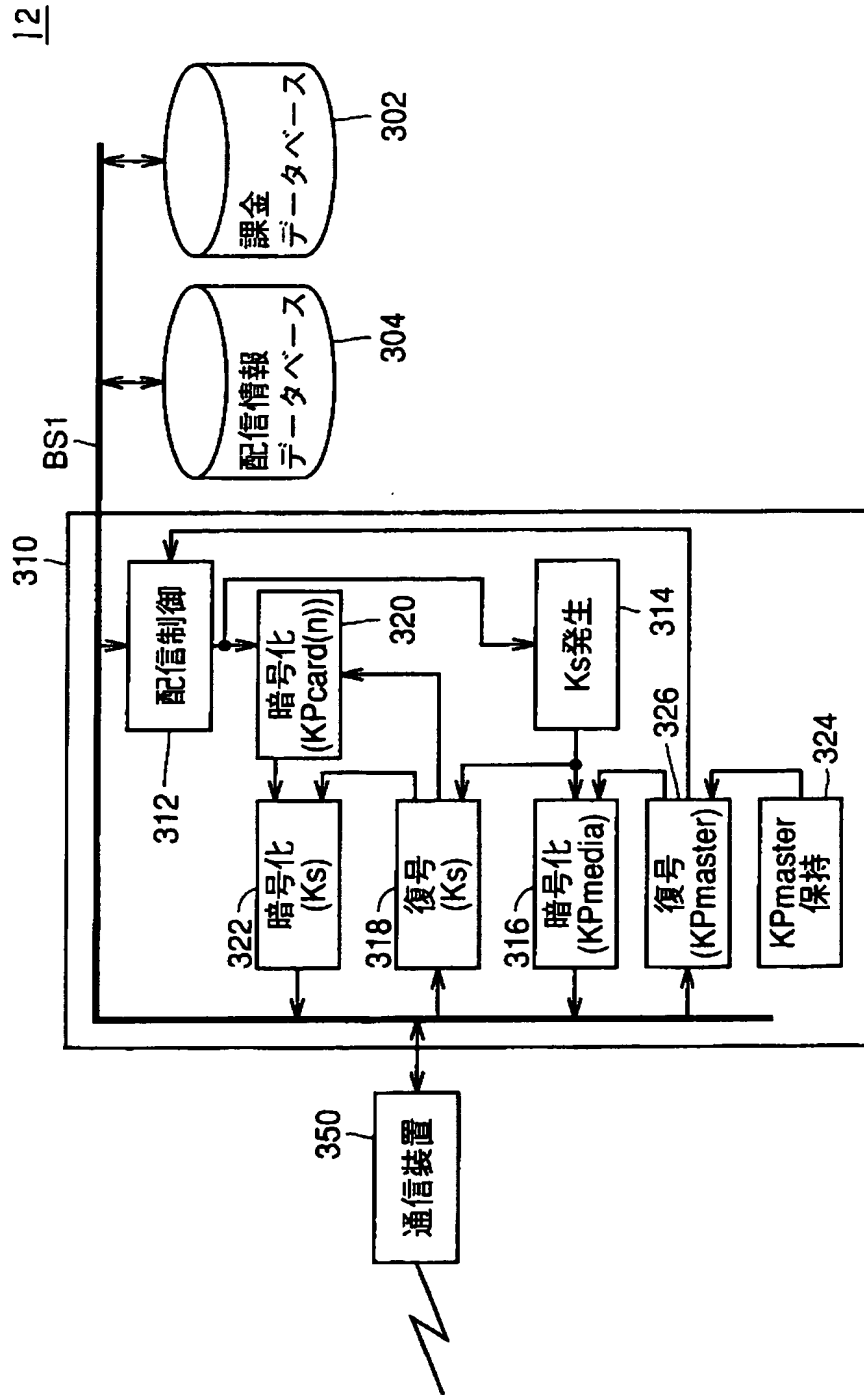
【図 3 1】



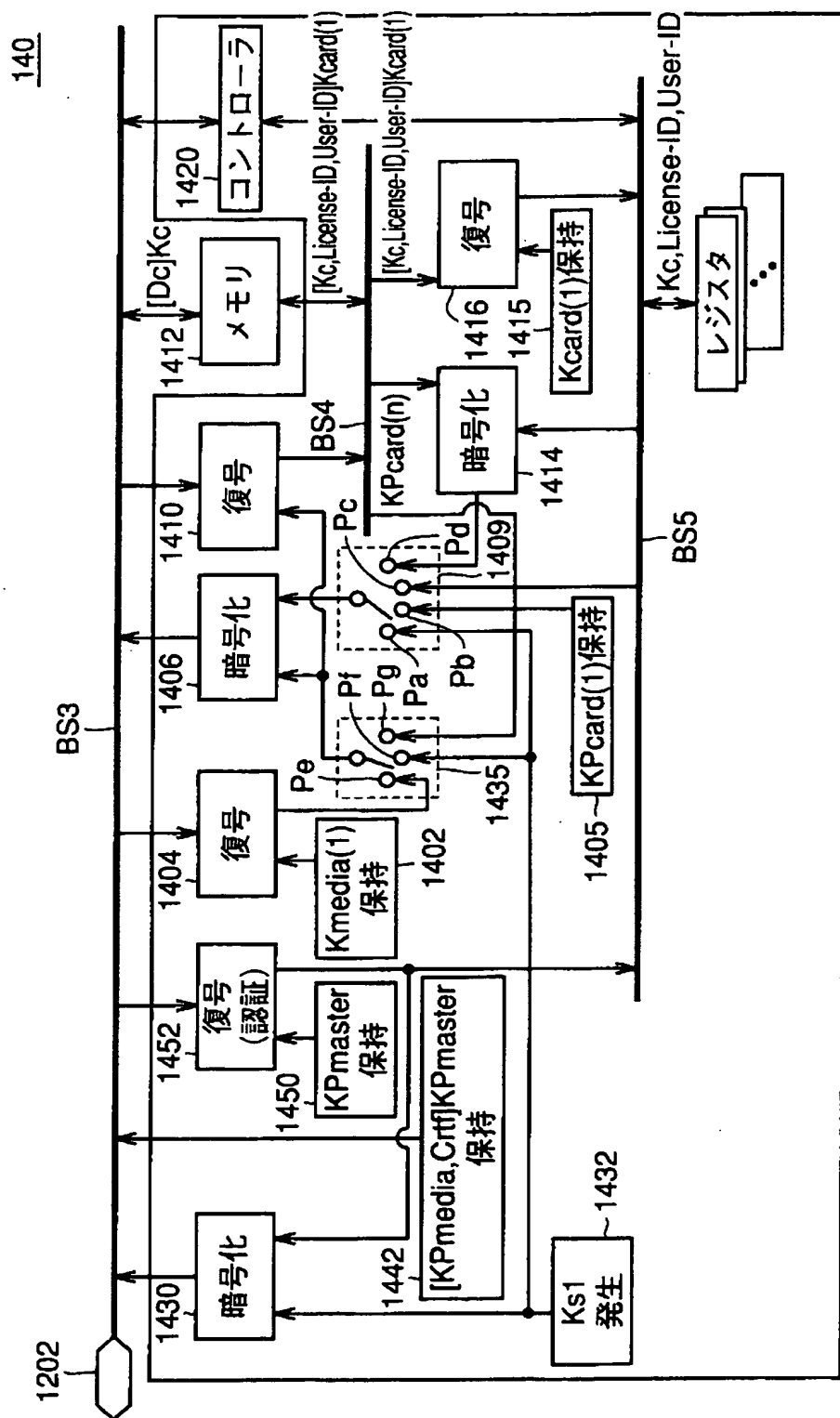
【図 3 2】



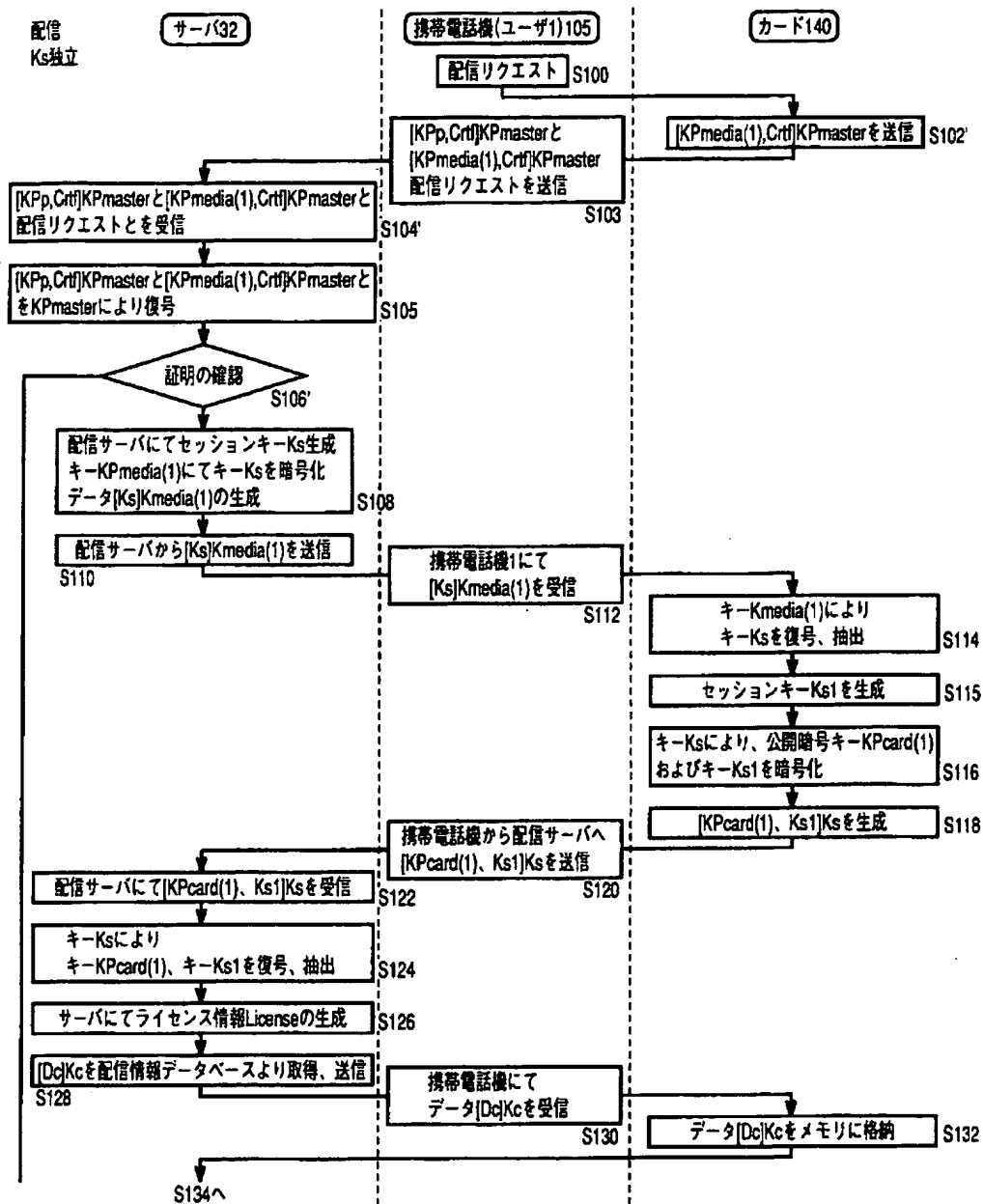
【図 3 3】



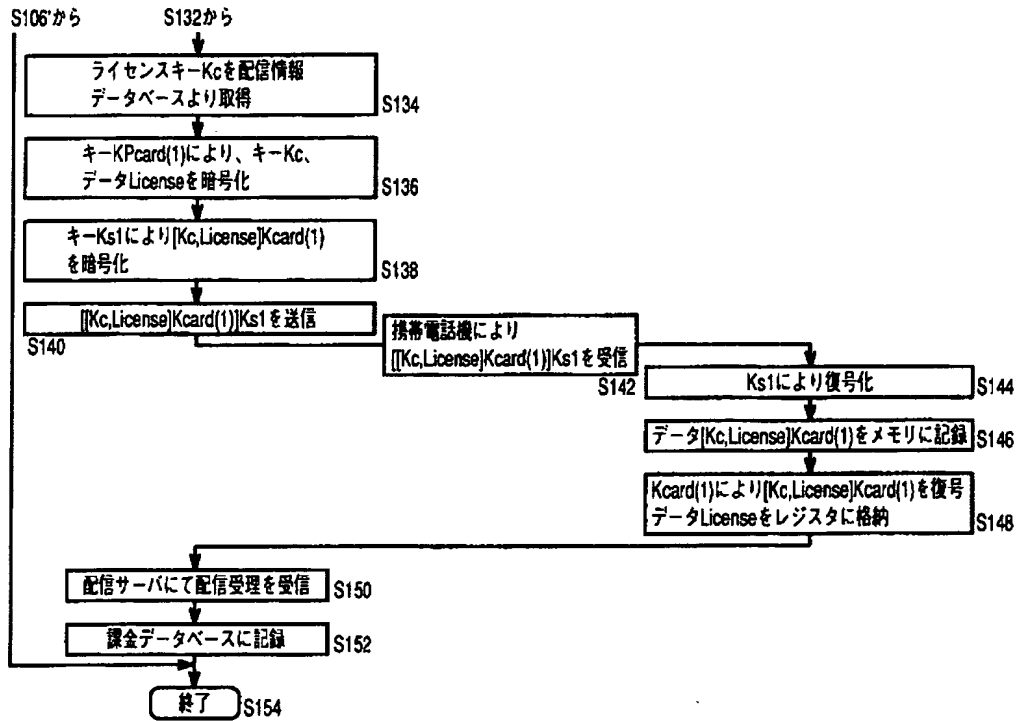
【図 3 4】



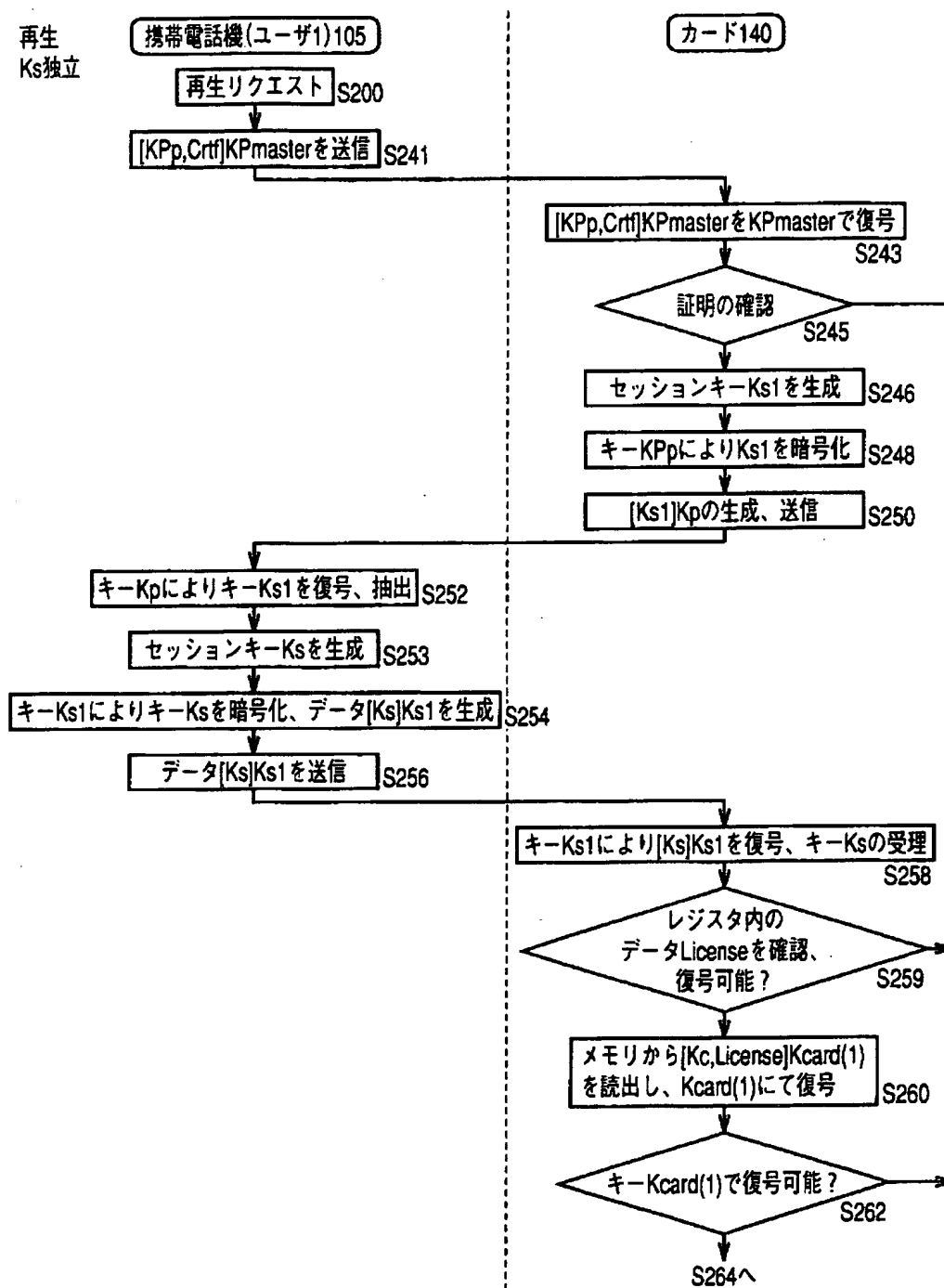
【図 3 5】



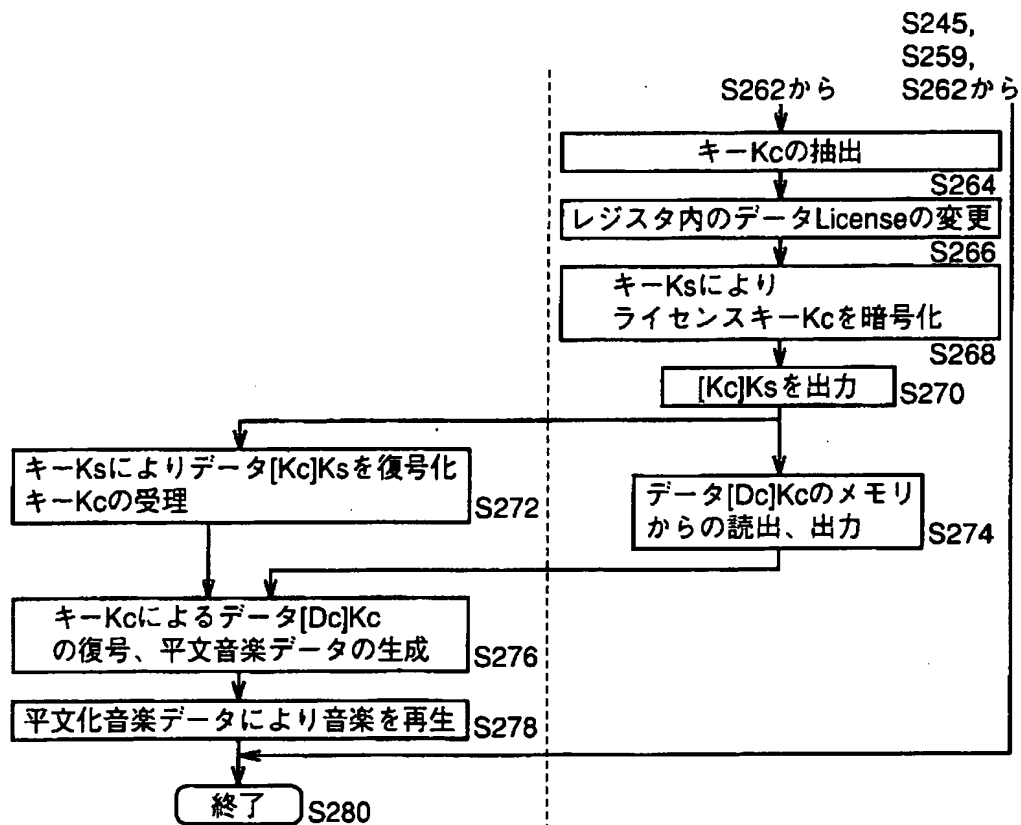
【図 3 6】



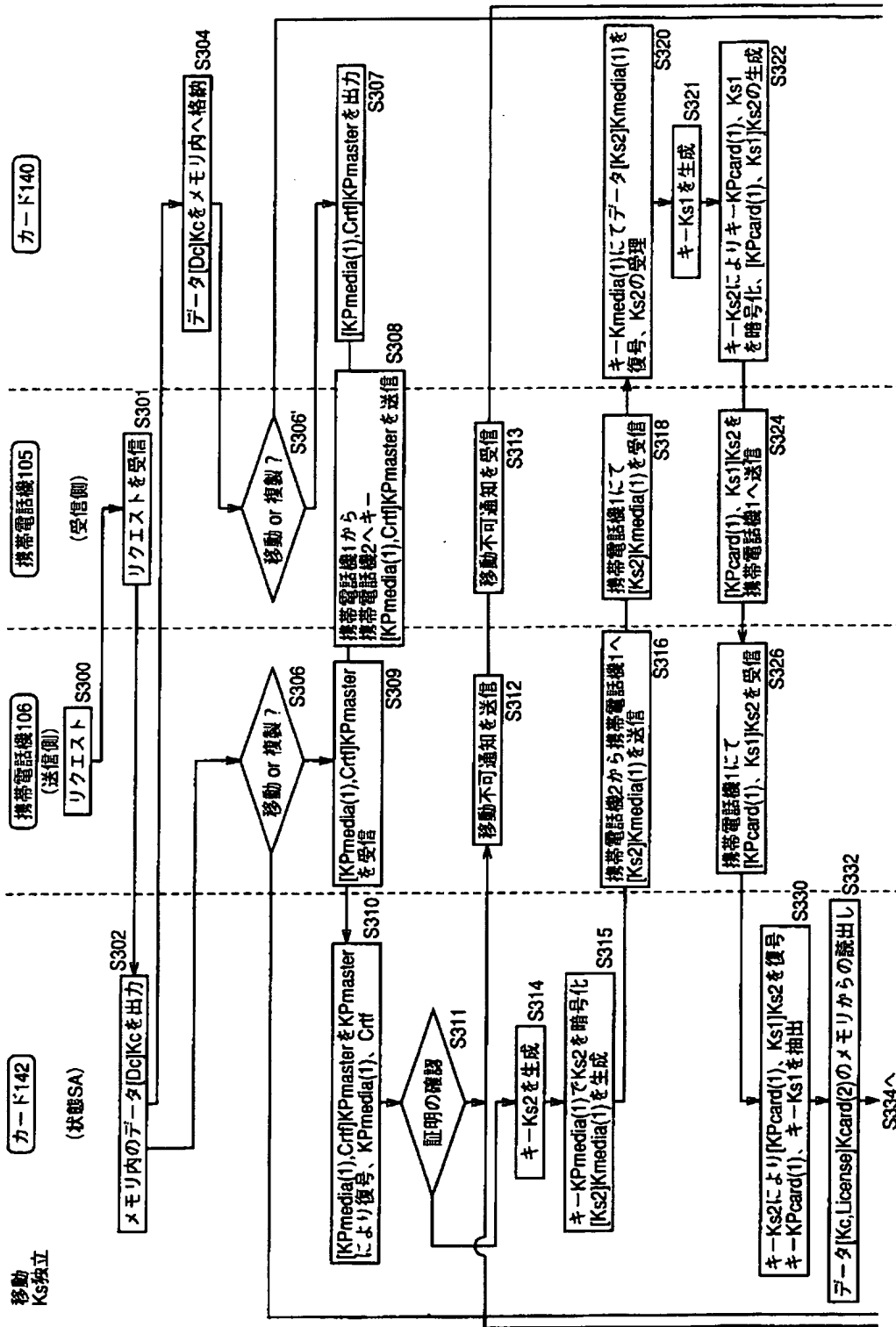
【図 3 7】



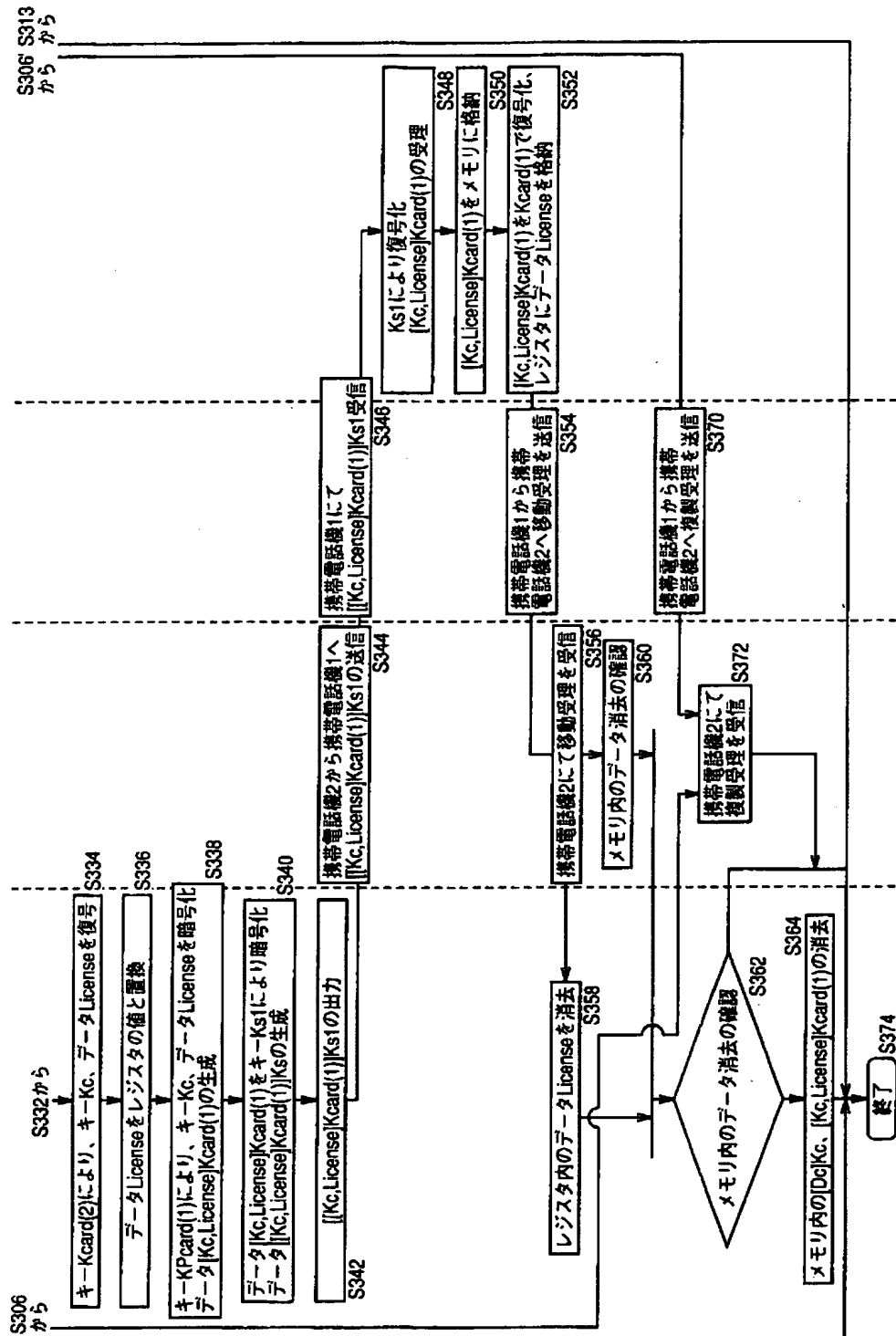
【図 3 8】



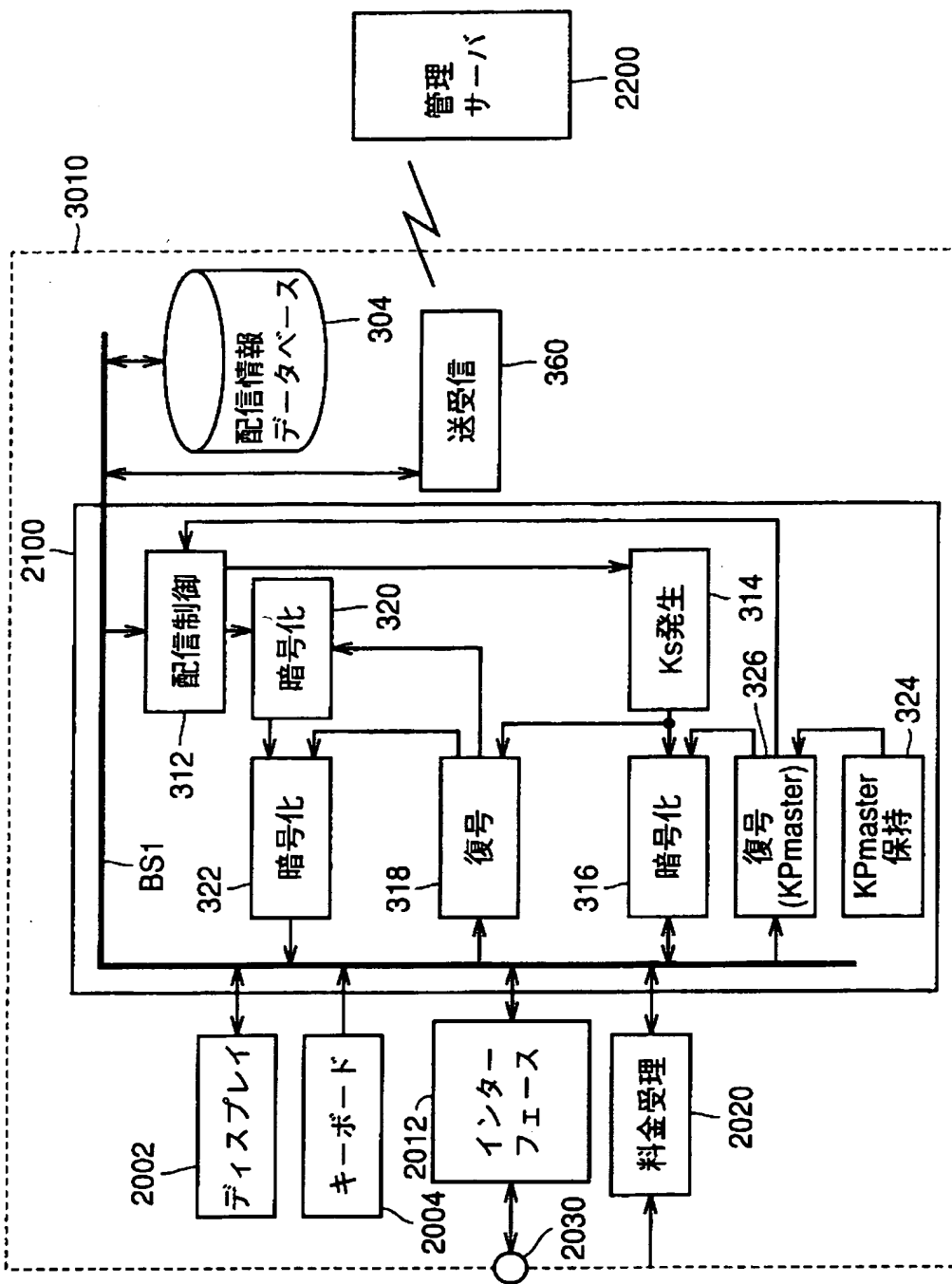
【図 3 9】



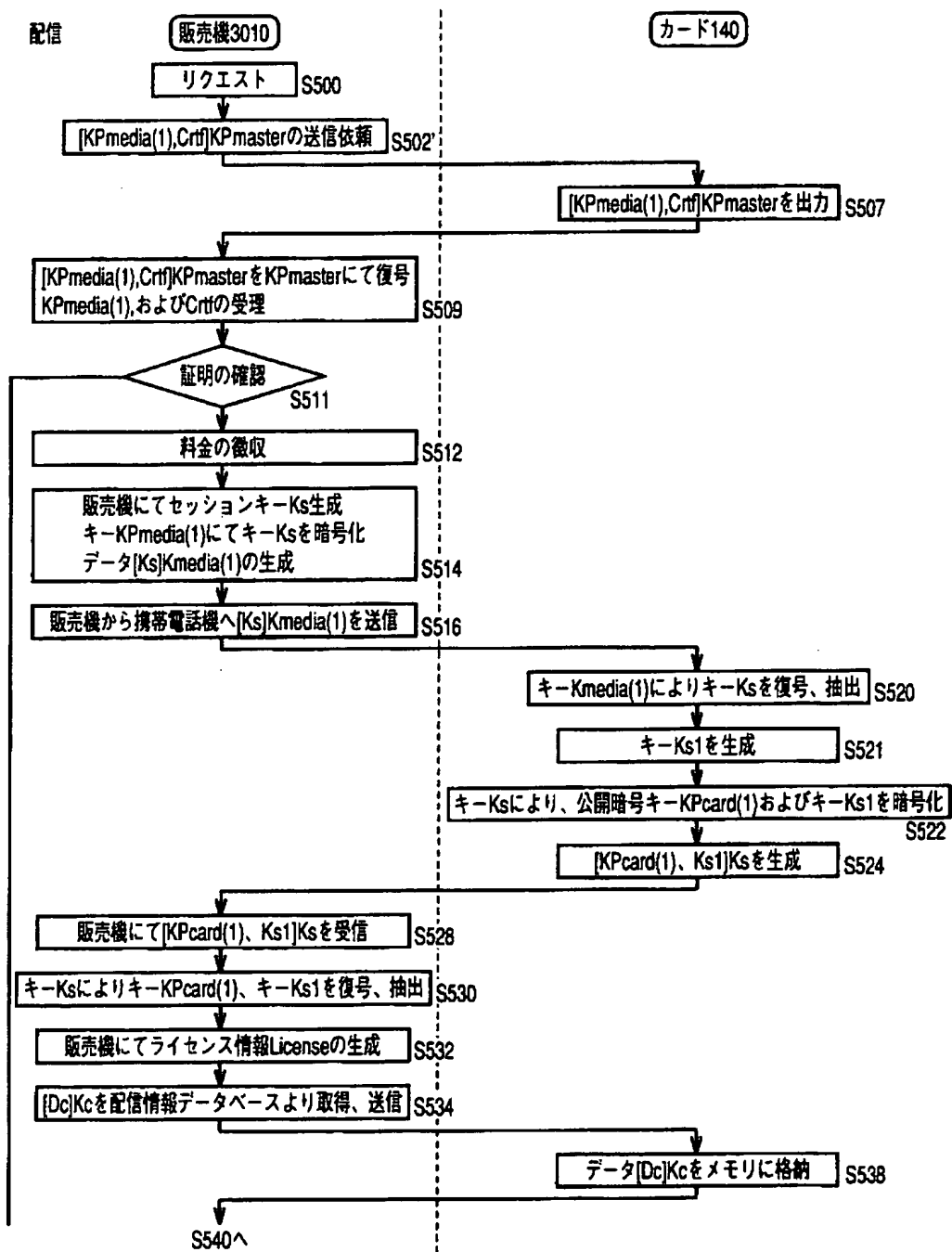
【図 4 0】



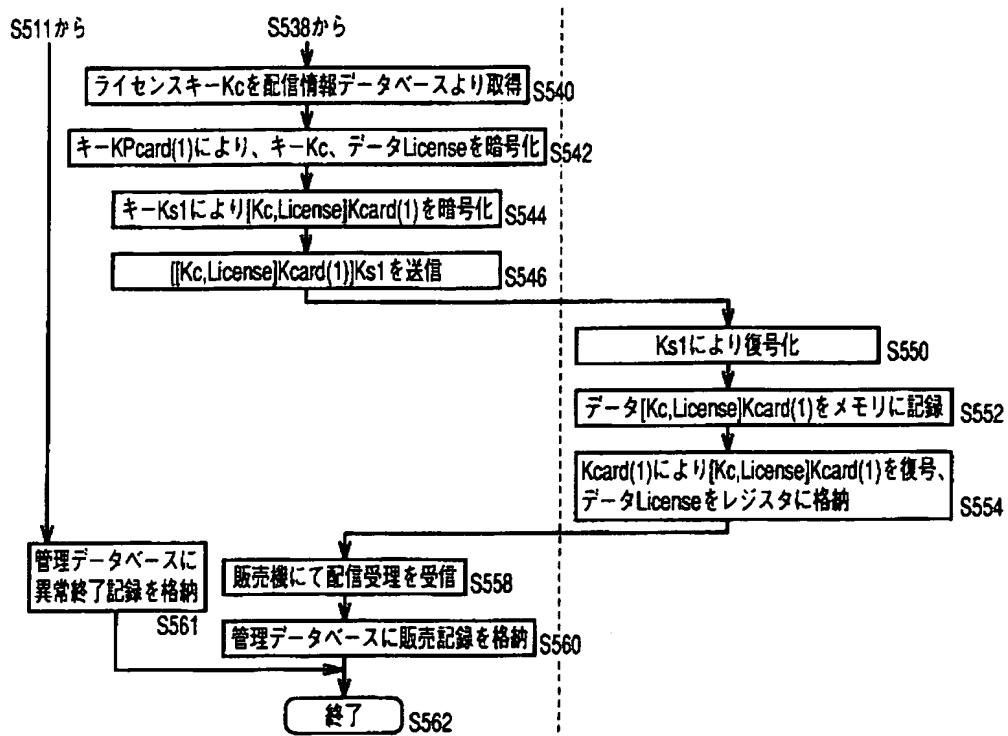
【図 4 1】



【図 4 2】

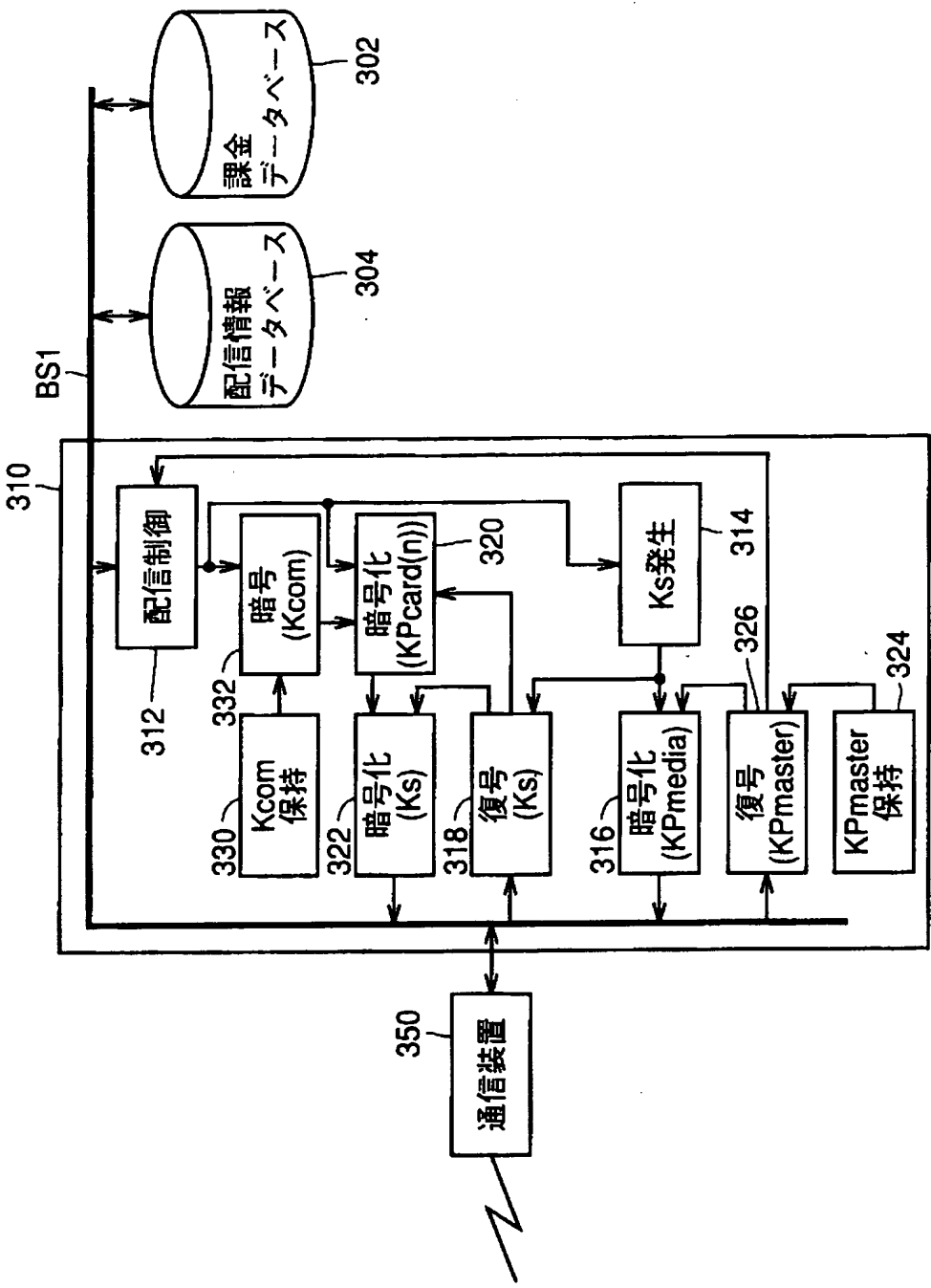


【図 4 3】

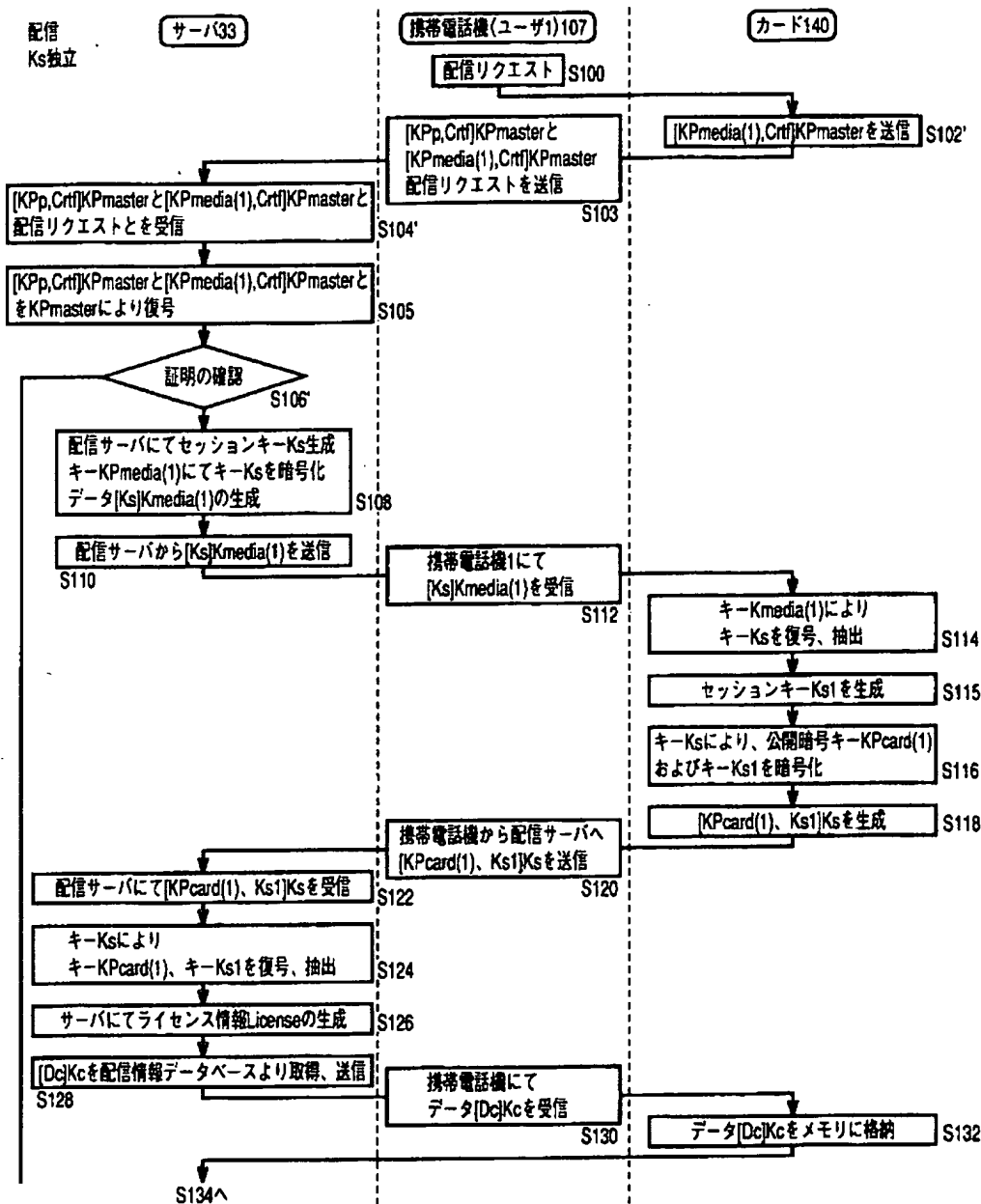


【図 4 5】

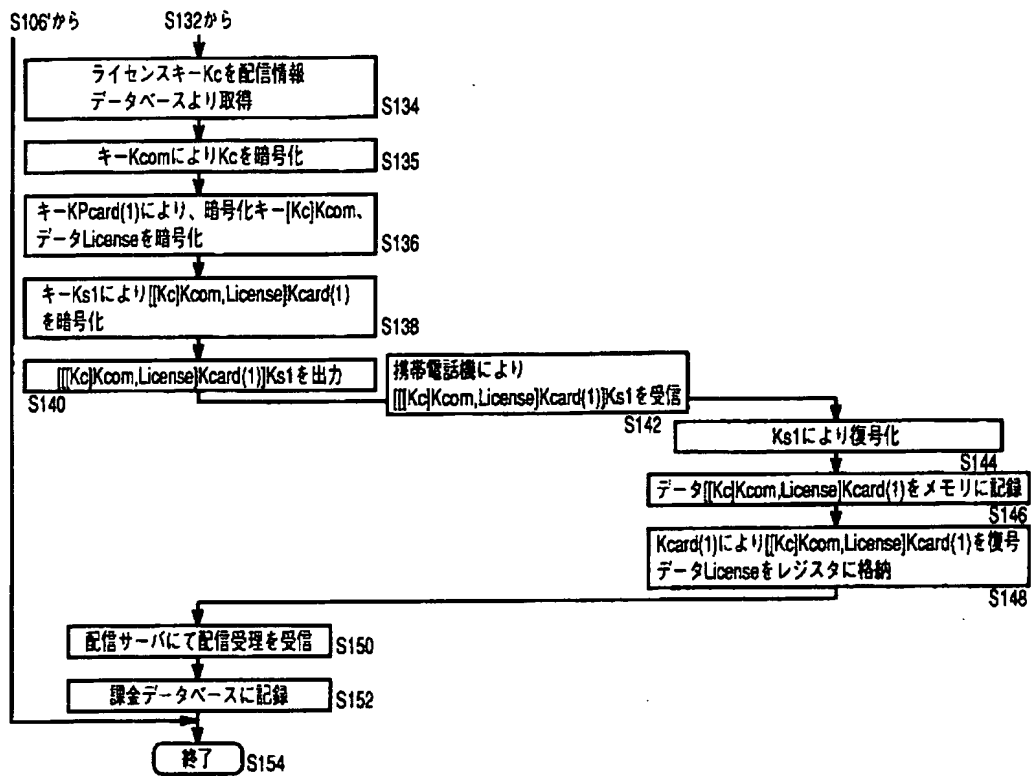
13



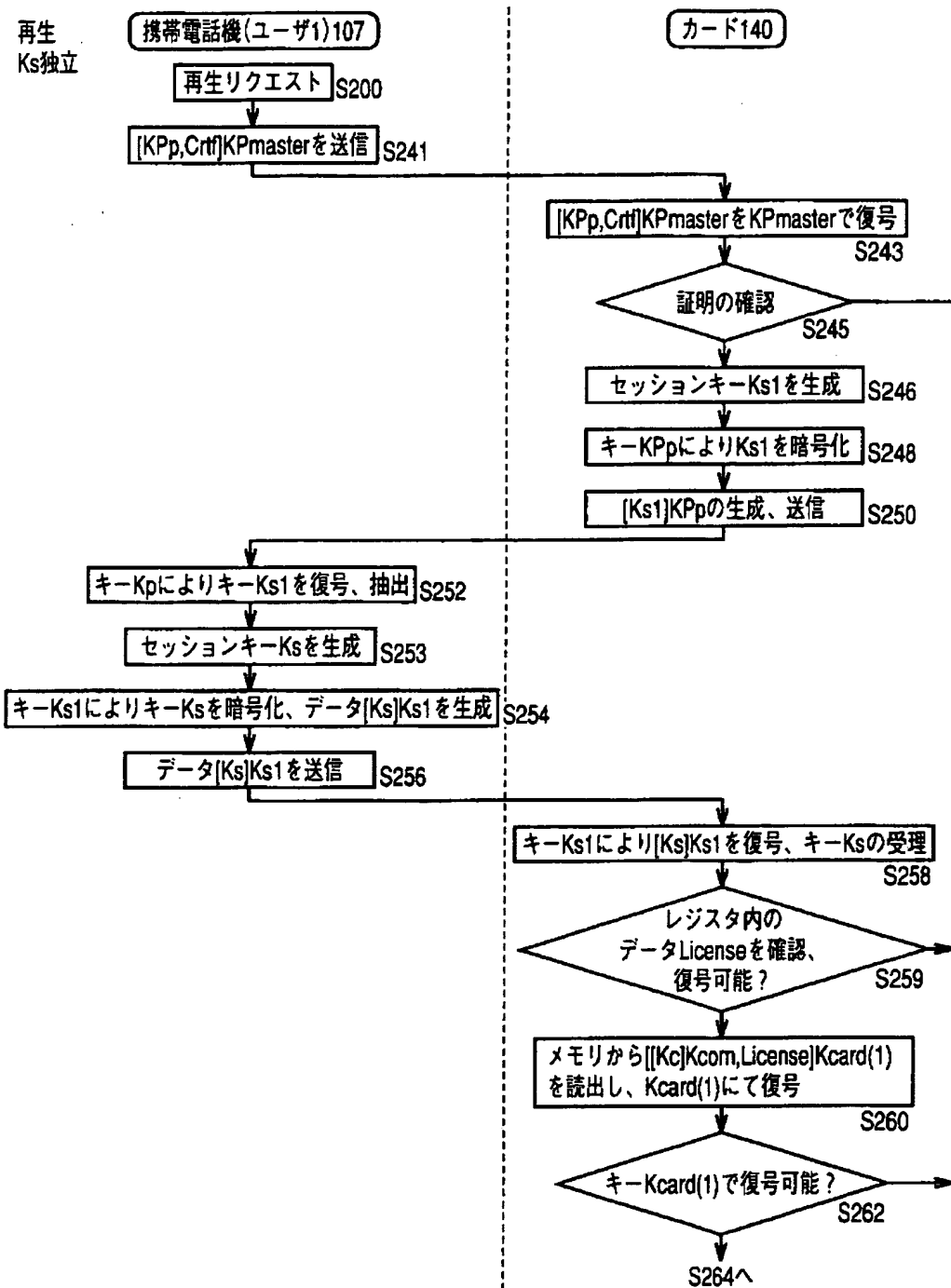
【図 4 6】



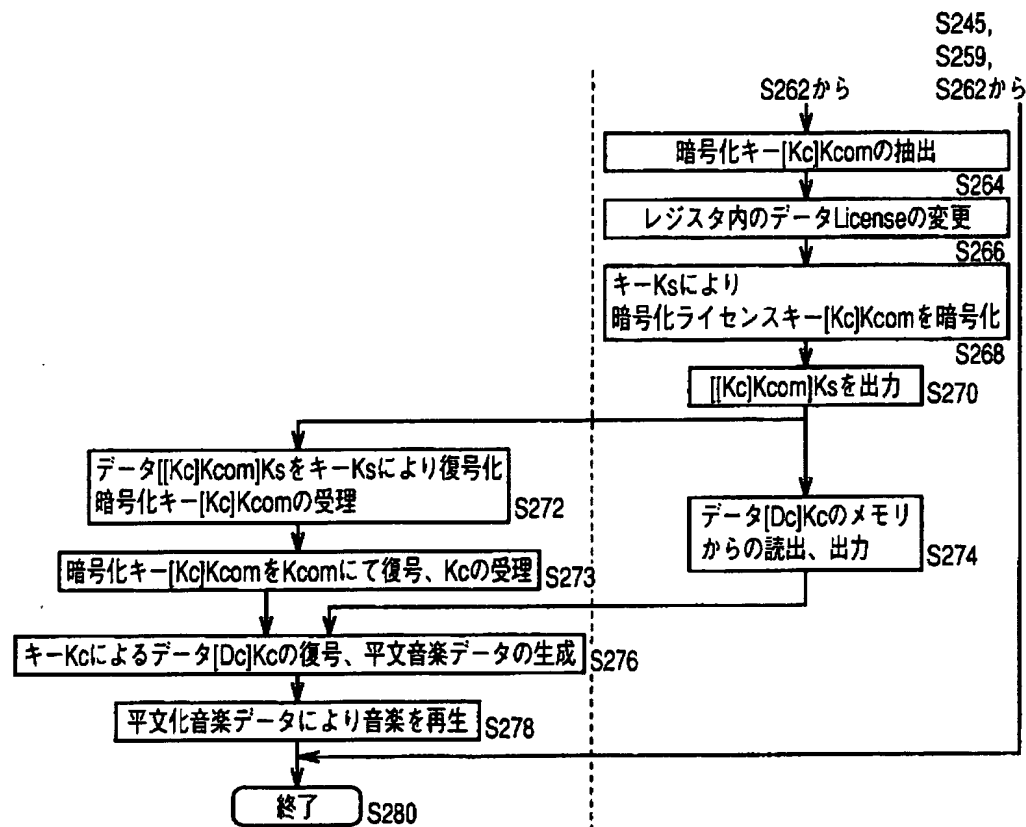
【図 4 7】



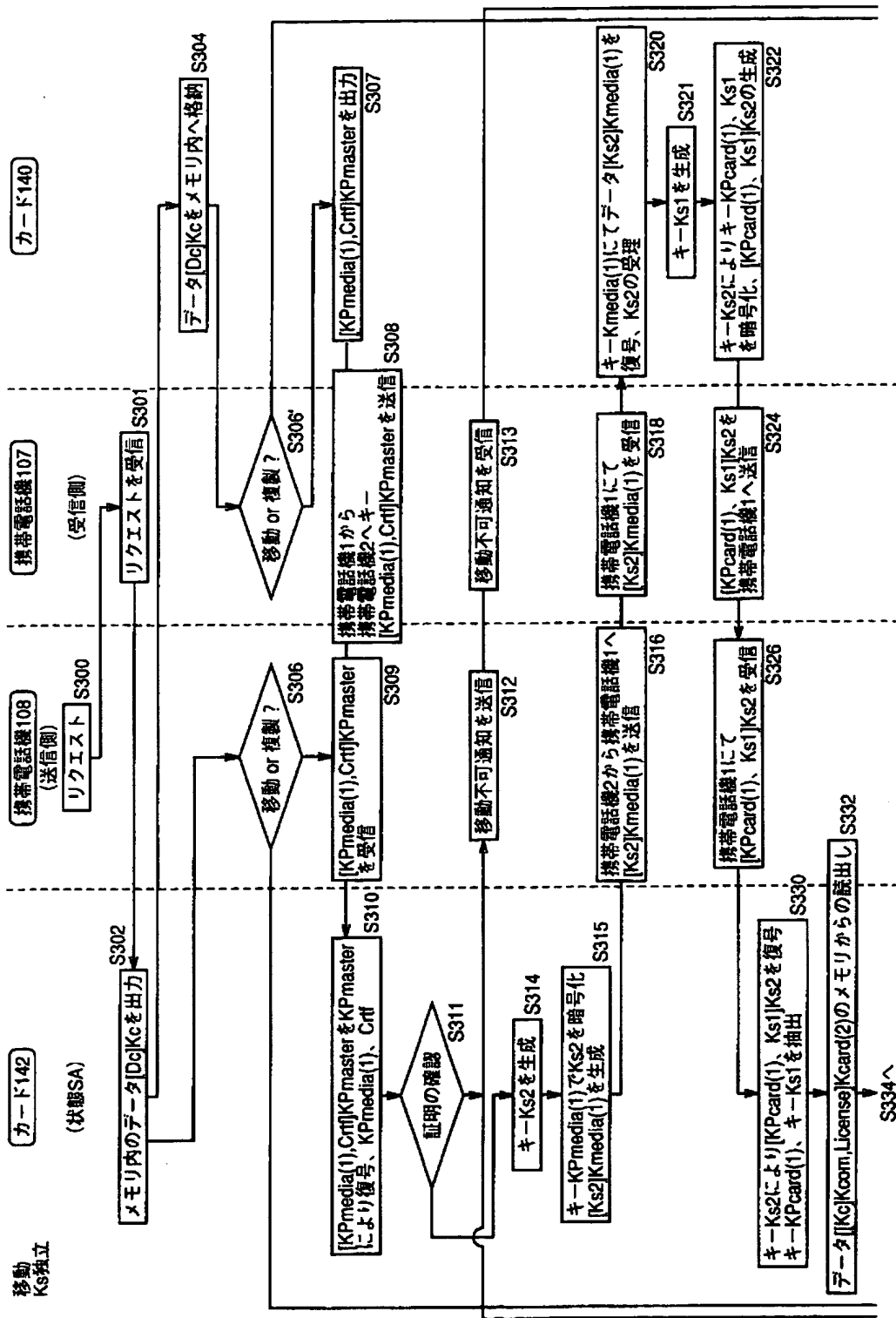
【図 4 8】



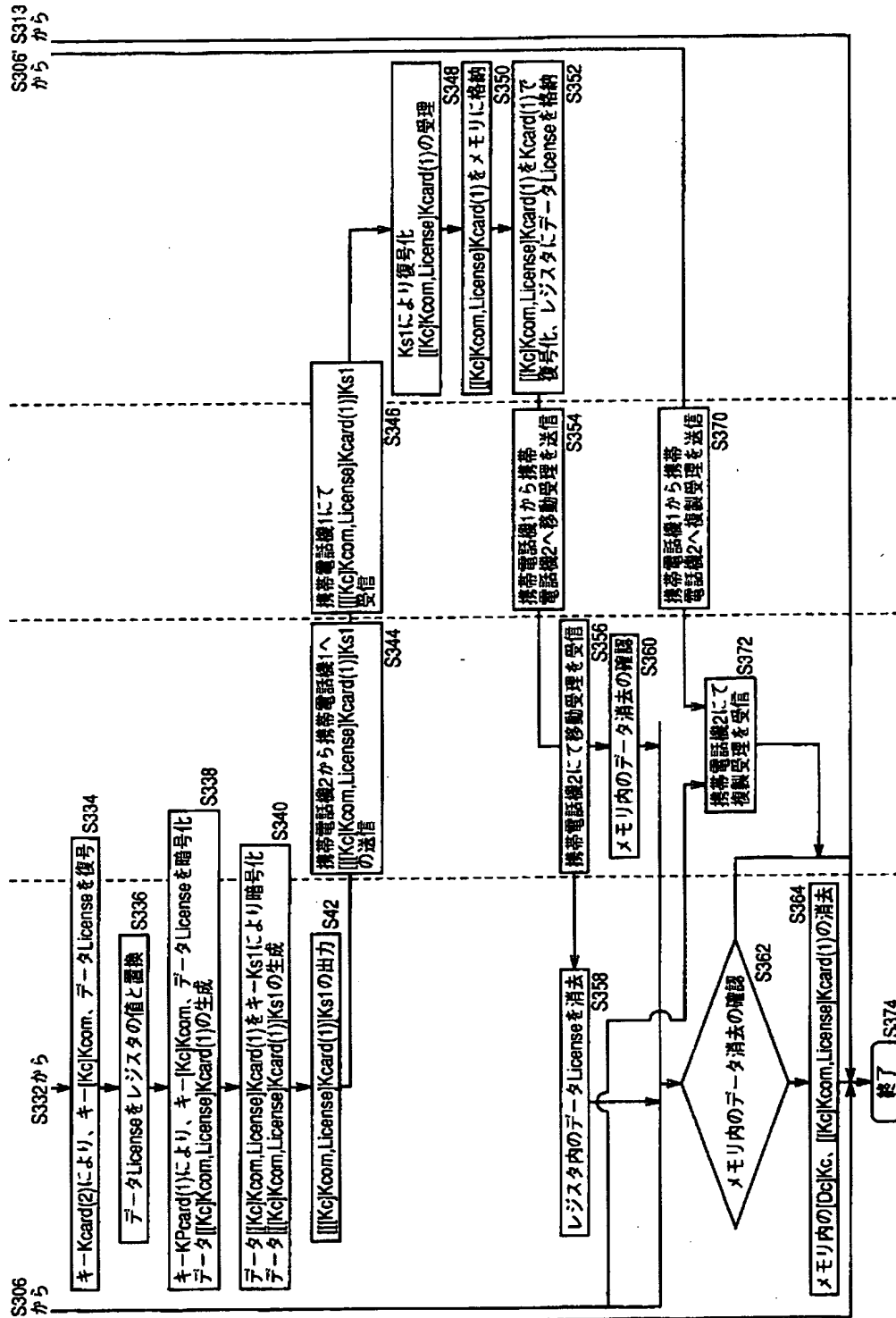
【図 4 9】



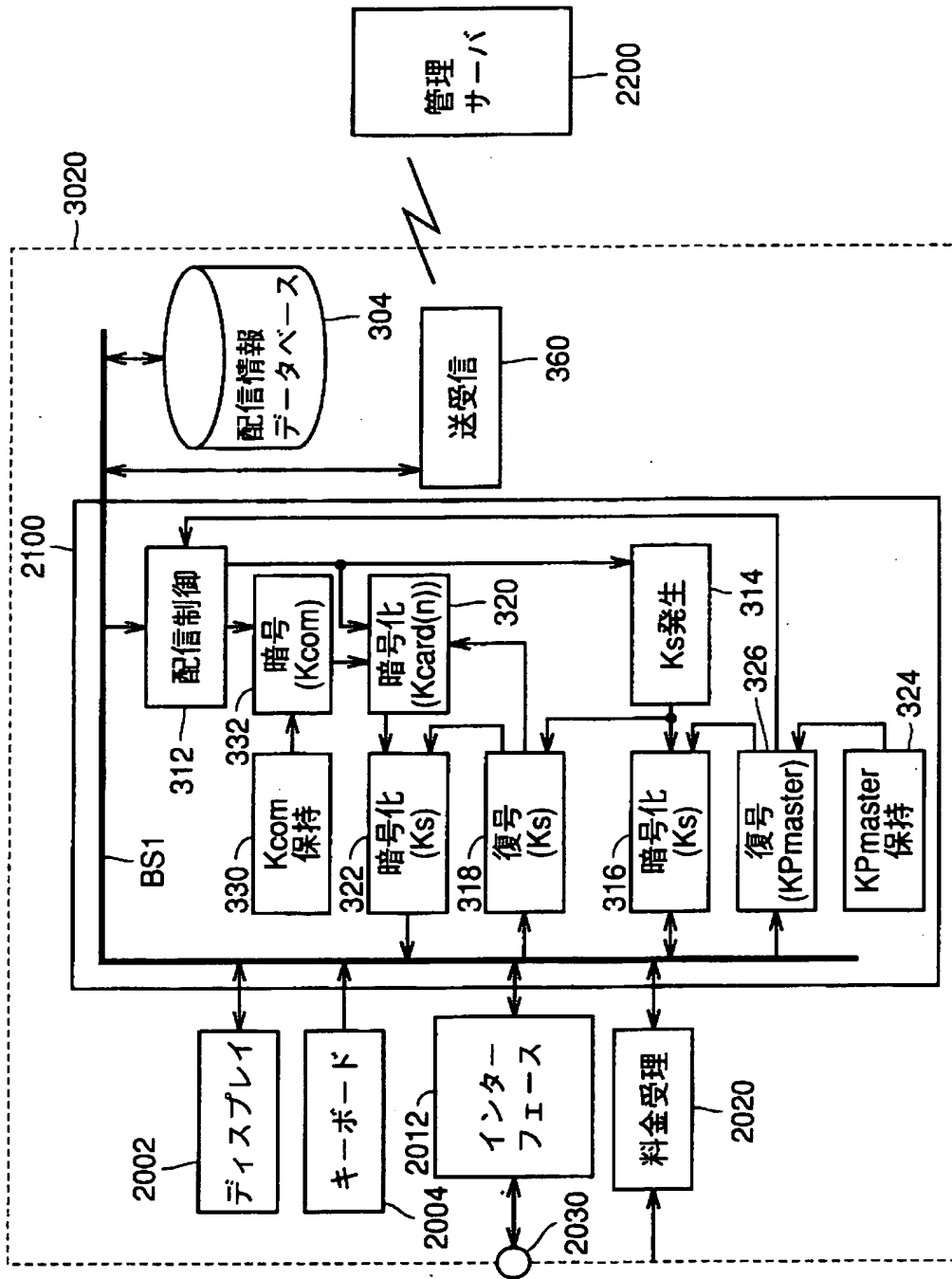
【図 50】



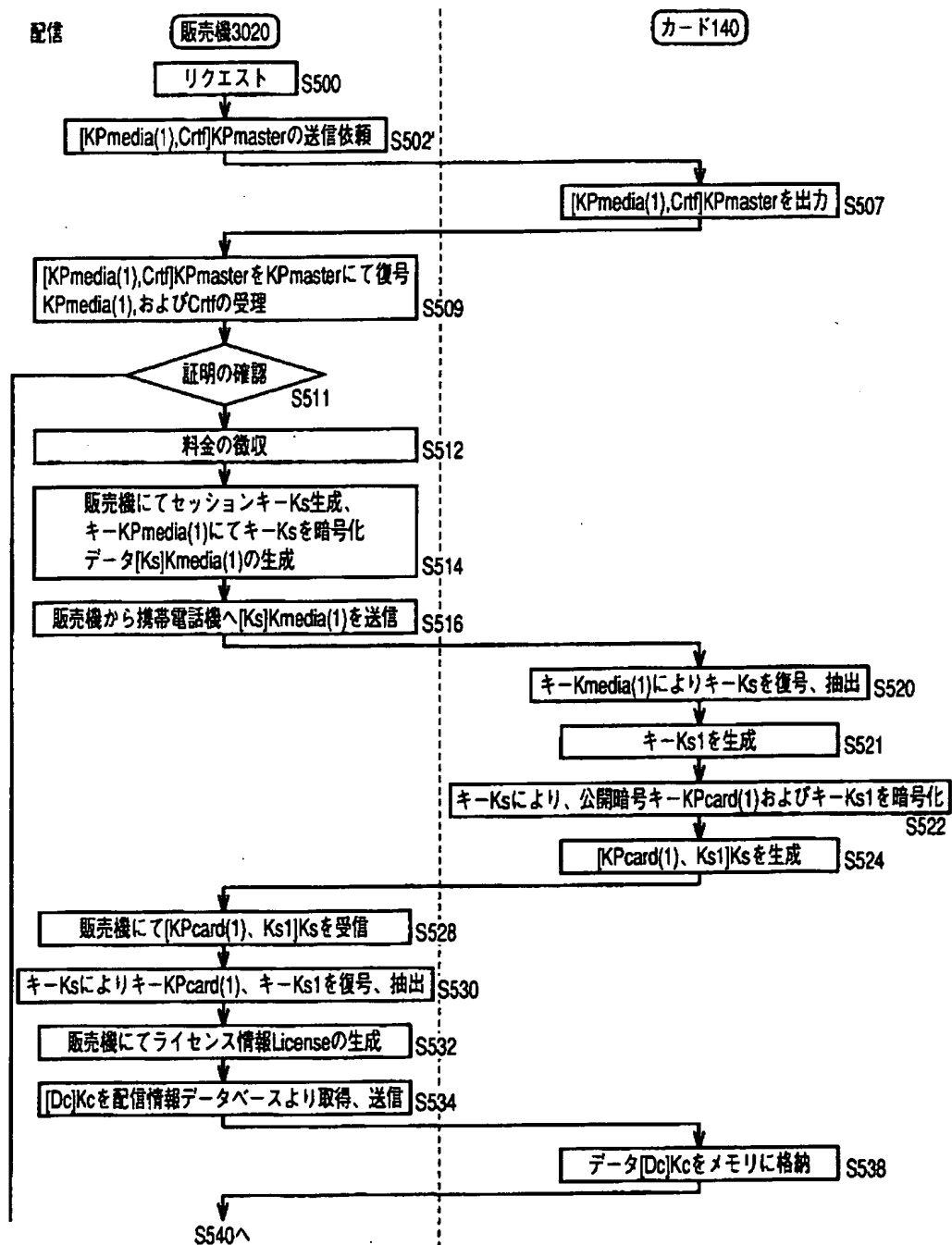
【図 5 1】



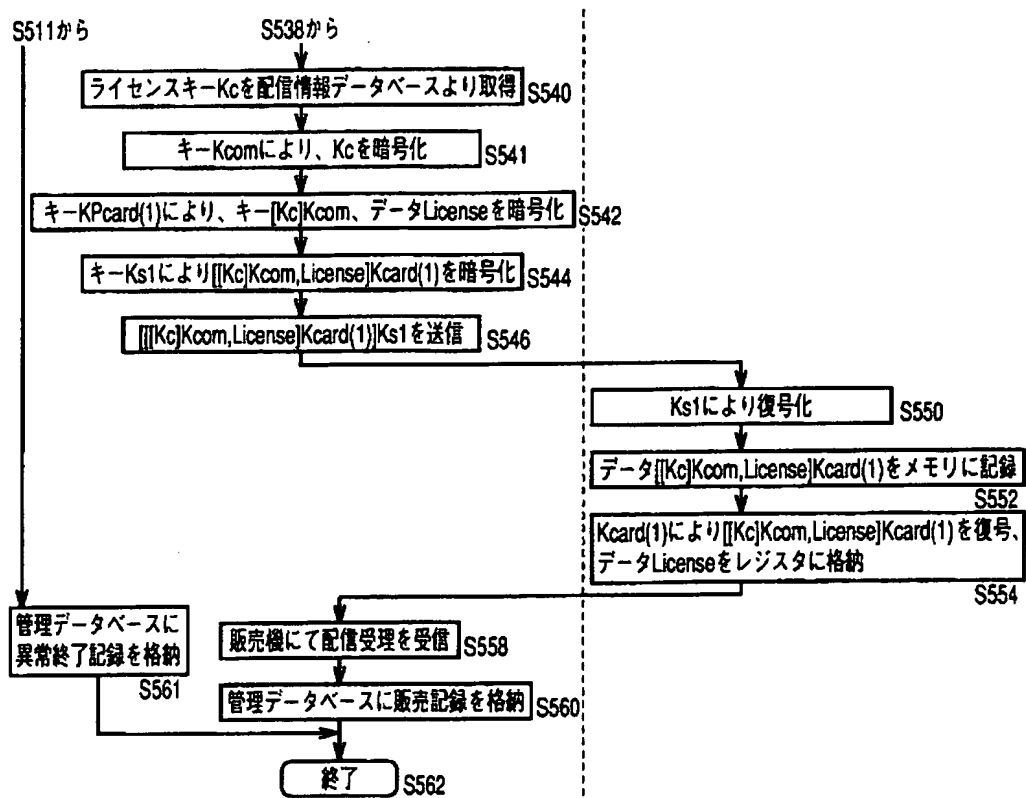
【図 5 2】



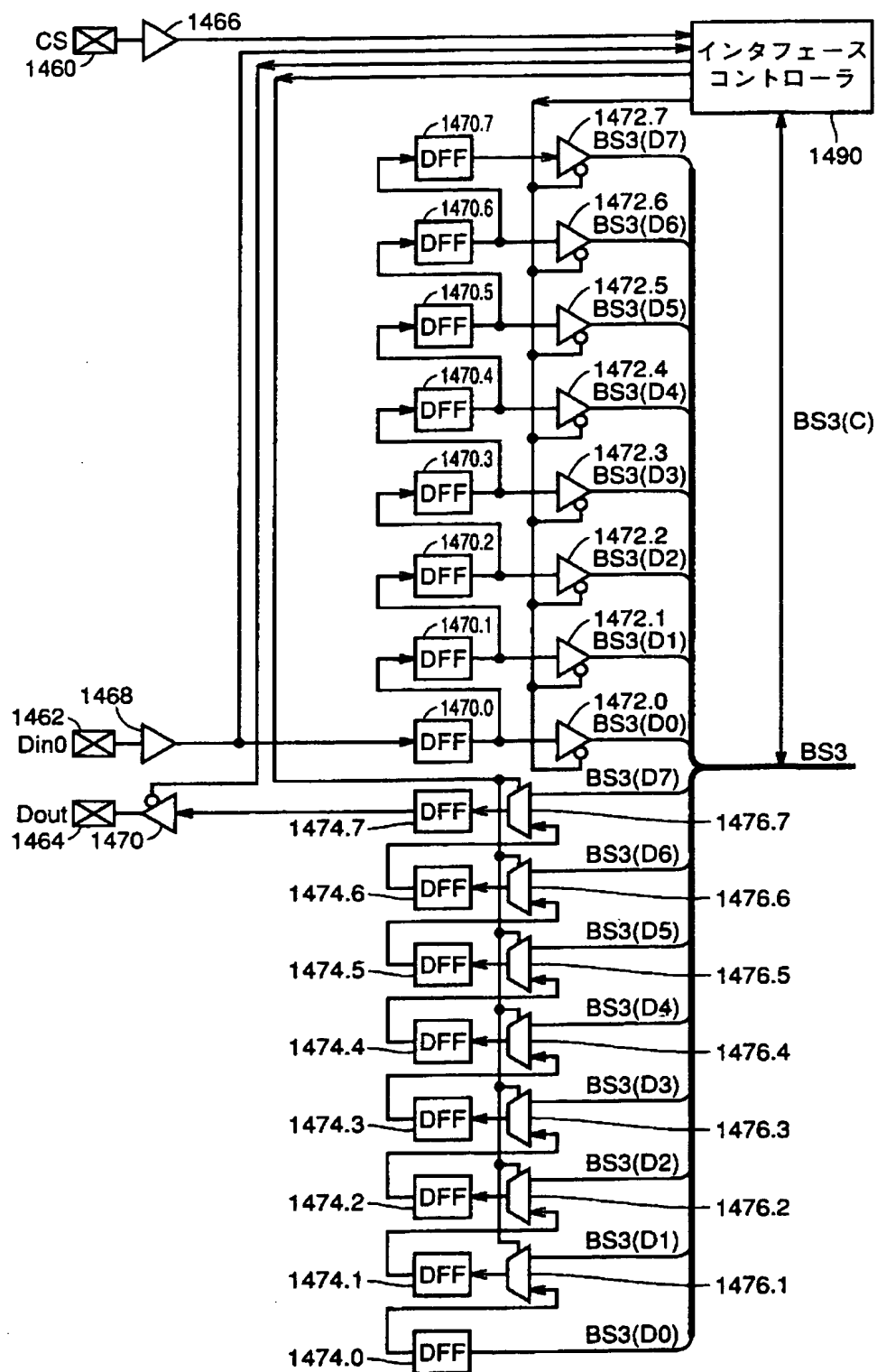
【図 5 3】



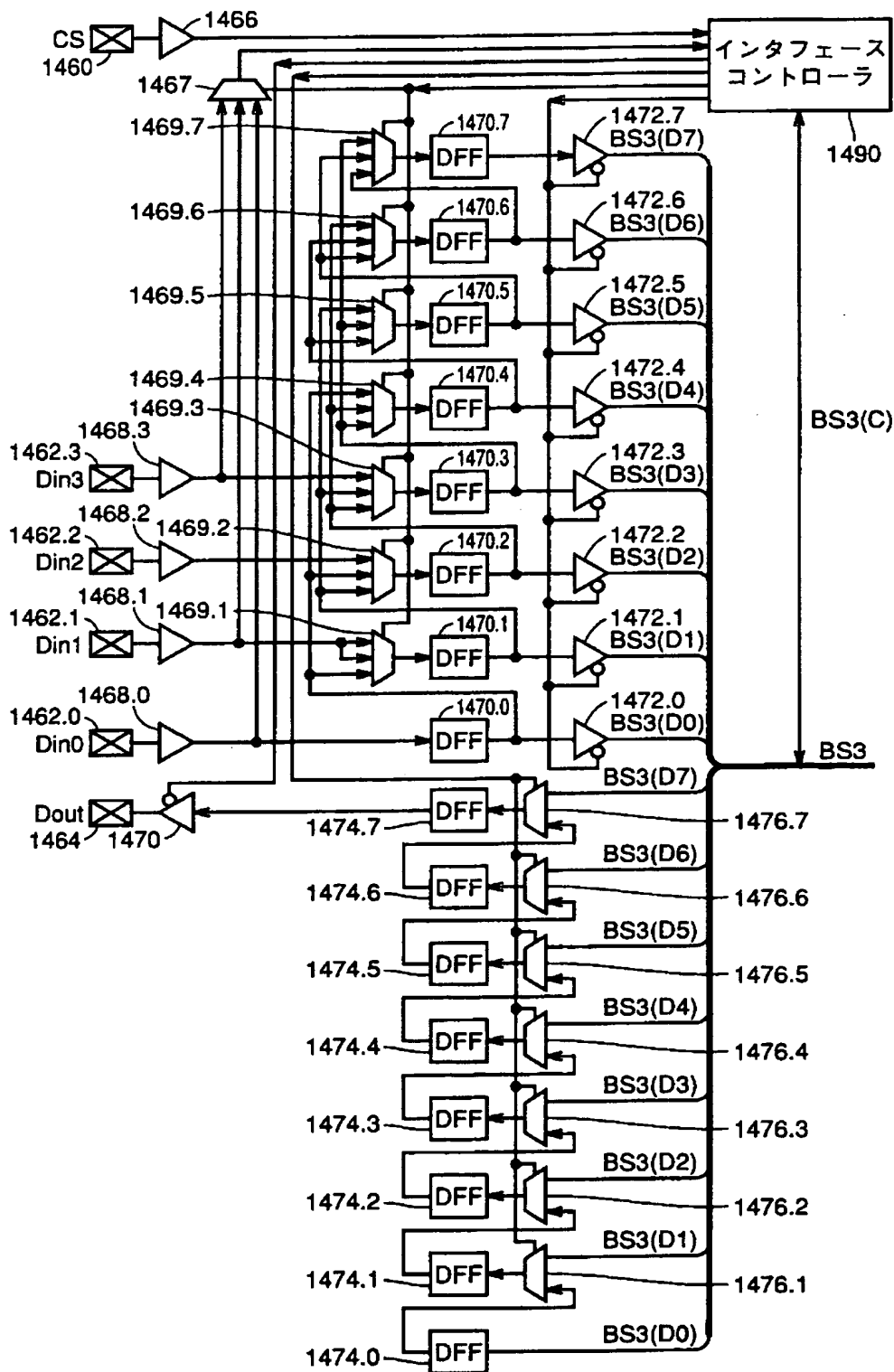
【図 5 4】



【図 5 5】



【図 5 6】



【書類名】 要約書

【要約】

【課題】 著作権者の許可なく複製されることを防止することが可能な情報配信システムを提供する。

【解決手段】 メモリカード 1 1 0 は、サーバから携帯電話網を介してデータベース B S 3 に与えられるデータから、復号処理をすることによりセッションキー K s を抽出する。暗号化処理部 1 4 0 6 は、セッションキー K s に基づいて、メモリカード 1 1 0 の公開暗号化鍵 K P c a r d (1) を暗号化してデータベース B S 3 を介してサーバに与える。レジスタ 1 5 0 0 は、復号されたライセンス I D、ユーザ I D 等のデータをサーバから受けとって格納し、メモリ 1 4 1 2 は、データベース B S 3 からライセンスキー K c により暗号化されている暗号化コンテンツデータ [D c] K c を受けて格納する。

【選択図】 図 5

認定・付加情報

特許出願の番号	平成 1 1 年 特許願 第 3 4 5 2 2 9 号
受付番号	5 9 9 0 1 1 8 3 9 9 8
書類名	特許願
担当官	塩崎 博子 1 6 0 6
作成日	平成 1 2 年 2 月 1 0 日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005223
【住所又は居所】	神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号
【氏名又は名称】	富士通株式会社

【特許出願人】

【識別番号】	000005108
【住所又は居所】	東京都千代田区神田駿河台四丁目 6 番地
【氏名又は名称】	株式会社日立製作所

【特許出願人】

【識別番号】	000004167
【住所又は居所】	東京都港区赤坂 4 丁目 1 4 番 1 4 号
【氏名又は名称】	日本コロムビア株式会社

【特許出願人】

【識別番号】	000001889
【住所又は居所】	大阪府守口市京阪本通 2 丁目 5 番 5 号
【氏名又は名称】	三洋電機株式会社

【代理人】

申請人	
【識別番号】	100064746
【住所又は居所】	大阪府大阪市北区南森町 2 丁目 1 番 2 9 号 住友 銀行南森町ビル 深見特許事務所
【氏名又は名称】	深見 久郎

【選任した代理人】

【識別番号】	100085132
【住所又は居所】	大阪府大阪市北区南森町 2 丁目 1 番 2 9 号 住友 銀行南森町ビル 深見特許事務所
【氏名又は名称】	森田 俊雄

【選任した代理人】

【識別番号】	100091409
--------	-----------

次頁有

認定・付加情報（続き）

【住所又は居所】 大阪府大阪市北区南森町 2 - 1 - 2 9 住友銀行
南森町ビル 深見特許事務所

【氏名又は名称】 伊藤 英彦

【選任した代理人】

【識別番号】 100096781

【住所又は居所】 大阪府大阪市北区南森町 2 - 1 - 2 9 住友銀行
南森町ビル 深見特許事務所

【氏名又は名称】 堀井 豊

次頁無

特願平 1 1 - 3 4 5 2 2 9

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 2 2 3]

1. 変更年月日 1 9 9 6 年 3 月 2 6 日

[変更理由] 住所変更

住 所 神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名 富士通株式会社

特願平 1 1 - 3 4 5 2 2 9

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 1 0 8]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日
[変更理由] 新規登録
住 所 東京都千代田区神田駿河台 4 丁目 6 番地
氏 名 株式会社日立製作所
2. 変更年月日 2 0 0 4 年 9 月 8 日
[変更理由] 住所変更
住 所 東京都千代田区丸の内一丁目 6 番 6 号
氏 名 株式会社日立製作所

特願平 1 1 - 3 4 5 2 2 9

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 4 1 6 7]

1. 変更年月日 1 9 9 0 年 8 月 2 1 日
[変更理由] 新規登録
住 所 東京都港区赤坂 4 丁目 1 4 番 1 4 号
氏 名 日本コロムビア株式会社
2. 変更年月日 2 0 0 2 年 1 0 月 2 2 日
[変更理由] 名称変更
住 所 東京都港区赤坂 4 丁目 1 4 番 1 4 号
氏 名 コロムビアミュージックエンタテインメント株式会社
3. 変更年月日 2 0 0 5 年 8 月 3 0 日
[変更理由] 住所変更
住 所 東京都港区六本木一丁目 4 番 3 3 号 六本木 2 1 森ビル
氏 名 コロムビアミュージックエンタテインメント株式会社

特願平 1 1 - 3 4 5 2 2 9

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 1 8 8 9]

1. 変更年月日 1 9 9 3 年 1 0 月 2 0 日

[変更理由] 住所変更

住 所 大阪府守口市京阪本通 2 丁目 5 番 5 号

氏 名 三洋電機株式会社